# Lemma for Linear Feedback Shift Registers and DFTs Applied to Affine Variety Codes

Hajime Matsui

**Abstract**

In this paper, we establish a lemma in algebraic coding theory that frequently appears in the encoding and decoding of, e.g., Reed-Solomon codes, algebraic geometry codes, and affine variety codes. Our lemma corresponds to the non-systematic encoding of affine variety codes, and can be stated by giving a canonical linear map as the composition of an extension through linear feedback shift registers from a Gröbner basis and a generalized inverse discrete Fourier transform. We clarify that our lemma yields the error-value estimation in the fast erasure-and-error decoding of a class of dual affine variety codes. Moreover, we show that systematic encoding corresponds to a special case of erasure-only decoding. The lemma enables us to reduce the computational complexity of error-evaluation from $O(n^3)$ using Gaussian elimination to $O(qn^2\log_q n)$ with some mild conditions on $n$ and $q$, where $n$ is the code length and $q$ is the finite-field size.

**Index Terms**

Gröbner bases, evaluation codes from order domains, fast decoding, systematic encoding, Berlekamp-Massey-Sakata algorithm.

## I. Introduction

Affine variety codes [8],[11],[17],[24] belong to a naturally generalized class of algebraic geometry (AG) codes, and are also known as evaluation codes from order domains of finitely generated types [1],[10],[15],[16]. It is known [8] that affine variety codes represent all linear codes. On the other hand, Pellikaan *et al.* [25] have already shown that AG codes, especially codes on algebraic curves, also represent all linear codes. Thus, from the viewpoint of code construction, one might consider only codes on algebraic curves. However, in terms of decoding, it is insufficient to focus only on AG codes, because many efficient decoding algorithms can correct errors up to half the generalized Feng–Rao minimum distance bound $d_{\mathrm{FR}}$ [4],[23],[27],[32], which depends on orders among vector basis or monomial basis. Whereas AG codes use a specified order, affine variety codes have the advantage that they can choose their orders flexibly, allowing them to reach potentially good $d_{\mathrm{FR}}$ values.

Manuscript submitted October 28, 2012. This work was supported in part by KAKENHI, Grant-in-Aid for Scientific Research (C) (23560478). The material in this paper was presented in part at the 34th Symposium on Information Theory and Its Applications, Ousyuku, Iwate, Japan, Nov. 29–Dec. 2, 2011.

H. Matsui is with Toyota Technological Institute, Hisakata 2–12–1, Tenpaku, Nagoya 468–0034, Japan (e-mail: matsui@toyota-ti.ac.jp).

Pellikaan [26] developed a decoding algorithm for all linear codes using a $t$-error correcting pair and solving a system of linear equations; its computational complexity is of the order $n^3$, where $n$ is the code length. On the other hand, Fitzgerald *et al.* [8] and Marcolla *et al.* [17] proposed decoding algorithms via the Gröbner basis that correct errors up to half the minimum distance $\lfloor (d_{\min} - 1)/2 \rfloor$ for affine variety codes; as this type of decoding belongs to the class of NP-complete problems [2], the strong suggestion is that the algorithms in [8],[17] do not run in polynomial time.

The decoding of dual affine variety codes up to $\lfloor (d_{\mathrm{FR}} - 1)/2 \rfloor$ can be divided into two steps, namely error-location and error-evaluation. For the error-location step, O'Sullivan [4],[7] gave a generalization of the Berlekamp–Massey–Sakata (BMS) algorithm for finding the Gröbner bases of error-locator ideals for affine variety codes. The computational complexity of this algorithm is $bn^2$ (where $b$ is the number of elements in the Gröbner bases), which is less than $n^3$. However, for the error-evaluation step in the decoding, no efficient method with a computational complexity of less than $n^3$ has been found. Although there is a method [15] for error-value estimation based on the generalization of the key equation, its relation to the BMS algorithm has not been clarified, as discussed in [15, page 15], and its computational complexity has not been determined. Another method that uses the inverse matrix of the proper transform was introduced by Saints *et al.* [29], but its computational complexity is of the order $n^3$, because the inverse matrix must be computed for each error-evaluation step per decoding. Thus, there is currently no efficient method for error-value estimation in conjunction with the BMS algorithm.

The contents of this paper can be divided into three parts. First, we realize a generalization of the $N$-dimensional ($N$-D) discrete Fourier transform (DFT) and its inverse (IDFT) over finite fields, where $N$ is a positive integer. Let $q$ be a prime power, $\mathbb{F}_q$ be the finite field of $q$ elements, $\mathbb{F}_q^{\times} = \mathbb{F}_q \backslash \{0\}$, $\left(\mathbb{F}_q^{\times}\right)^N$ be the set of all $N$-tuples of elements in $\mathbb{F}_q^{\times}$, and $\mathbb{F}_q^N$ be similar to $\left(\mathbb{F}_q^{\times}\right)^N$. Whereas the conventional $N$-D DFT and IDFT over finite fields are defined upon vectors whose components are indexed by $\left(\mathbb{F}_q^{\times}\right)^N$, our generalized transforms are defined upon vectors whose components are indexed by $\mathbb{F}_q^N$, and agree with the conventional ones if they are restricted to $\left(\mathbb{F}_q^{\times}\right)^N$. In particular, our generalized transforms satisfy the Fourier inversion formulae; the inclusion-exclusion principal plays an essential role in their proofs. Secondly, we prove a lemma, which we call Main Lemma, concerning the linear feedback shift registers made by Gröbner bases and the generalized IDFT. Main Lemma provides a canonical isomorphic map from one vector space, consisting of vectors whose components are indexed by $D(\Psi)$, onto another vector space consisting of vectors whose components are indexed by $\Psi$. Here, for any subset $\Psi$ of $\mathbb{F}_q^N$, $D(\Psi)$ is the delta set (or footprint) of the Gröbner basis for an ideal of $N$-variable polynomials over $\mathbb{F}_q$ that have zeros at $\Psi$. Although these two vector spaces have the same dimension and are obviously isomorphic, our Main Lemma asserts that there is a canonical one-to-one map that does not depend on the choice of the bases of the vector spaces. This canonical isomorphic map can be explicitly written as the composition of the generalized IDFT after a map coming from the linear recurrence relations given by the Gröbner bases. The inverse of this canonical isomorphic map agrees with the proper transform introduced by Saints *et al.* [29].

Finally, Main Lemma is applied to affine variety codes in the following three topics. The first is the construction of affine variety codes, specifically their non-systematic encoding. Usually, the parity check matrices of affine variety codes must be derived from their generator matrices through matrix elimination. Using Main Lemma, we directly construct the dual affine variety codes as images of the canonical isomorphic map; this is analogous to the direct construction of affine variety codes as the images of the evaluation map. The second topic is the error-value estimation in the fast erasure-and-error decoding of a class of dual affine variety codes. We show that there is an efficient error-value estimation in conjunction with the BMS algorithm. Our method corresponds to a generalization of the methods of Sakata *et al.* [30],[31] for error-value estimation by DFT in case of one-point AG codes from algebraic curves, a subclass of AG codes. The final topic is the systematic encoding of the class of dual affine variety codes and the improved erasure-correcting capability. If a linear code has a non-trivial automorphism group, then it can be encoded systematically by the method of Heegard *et al.* [12] and Little [16]. Our systematic encoding does not use any automorphism group, and is applicable to a sufficiently wide class of dual affine variety codes. Moreover, we reveal that systematic encoding is a special type of erasure-only decoding; this fact is well-known in the case of maximum-distance codes [3], and is shown for the class of dual affine variety codes.

The contents of this paper are original, except for the definition of proper transforms [29], the definition of affine variety codes [8], and the error-value estimation of AG codes [30],[31]. The other contents are still original, even for the limited case of AG codes. Furthermore, if one adopts the conventional $N$-D DFT and IDFT over $\left(\mathbb{F}_q^{\times}\right)^N$ in place of our generalized transforms, then our Main Lemma and its applications to a subclass of dual affine variety codes are specialized for those in [22].

As mentioned above, because the isomorphic map of Main Lemma is equivalent to the inverse map of the proper transform in [29], the above applications to affine variety codes can also be performed by multiplying by the inverse matrix of the proper transform. Nevertheless, our IDFT-based expression of the inverse map enables us to reduce the computational complexity; moreover, this can be reduced further by applying a multidimensional DFT algorithm or FFT. Whereas the computational complexity of the error-value estimation with Gaussian elimination is of the order $n^3$, that with the proposed method has an upper bound of the order $nNq^N$, which is equivalent to $qn^2 \log_q n$ because $N$ can be chosen as $q^{N-1} < n \leq q^N$. Thus, our generalized IDFT and Main Lemma are not only important in the theory of affine variety codes, but are also useful in reducing the computational complexity of their error-value estimation.

The rest of this paper is organized as follows. In Section II, we prepare some notation for the subsequent discussions. Section III gives a generalization of DFTs from $\left(\mathbb{F}_q^{\times}\right)^N$ to $\mathbb{F}_q^N$. In Section IV, we state Main Lemma; Subsection IV-A defines two vector spaces via Gröbner bases, Subsection IV-B defines the map from the linear feedback shift registers given by Gröbner bases, and Subsection IV-C gives an isomorphism between the two vector spaces. In Section V, we apply the lemma to construct affine variety codes, reformulate erasure-and-error decoding algorithms, and determine the relation between systematic encoding and erasure-only decoding. In Section VI, we estimate the number of finite-field operations in our algorithm; Subsection VI-A uses a simple count and Subsection VI-B applies a multidimensional DFT algorithm. Section VII concludes the paper.

## II. Notation

Throughout this paper, the following notation is used. Let $\mathbb{N}_0$ be the set of non-negative integers. For $a, b \in \mathbb{N}_0$ with $a \le b$, let $[a,b] = \{a, a+1, \cdots, b\}$. For two sets $A$ and $B$, a set $A \backslash B$ is defined as $\{u \in A \,|\, u \notin B\}$. For an arbitrary finite set $S$, the number of elements in $S$ is represented by $|S|$, and let $V_S = \{(v_s)_S \mid s \in S, \, v_s \in \mathbb{F}_q\}$ denote an $|S|$-dimensional vector space over $\mathbb{F}_q$ whose components are indexed by elements of $S$. Unless otherwise noted, for any arbitrary subset $R \subseteq S$, the vector space $V_R$ is considered to be a subspace of $V_S$ given by $V_R = \{(v_s)_S \in V_S \mid v_s = 0 \text{ for all } s \in S\backslash R\}$. A map $f$ from a set $A$ into a set $B$ is represented by

$$f : A \to B \quad [a \mapsto f(a)] \,.$$

## III. Fourier-Type Transforms on $\mathbb{F}_q^N$

Let $N$ be a positive integer and let

$$A = [0, q-1]^N = \{ \underline{a} = (a_1, \cdots, a_N) \mid a_1, \cdots, a_N \in [0, q-1] \} \,,$$
$$\Omega = \mathbb{F}_q^N = \{ \underline{\omega} = (\omega_1, \cdots, \omega_N) \mid \omega_1, \cdots, \omega_N \in \mathbb{F}_q \} \,.$$

In this section, Fourier-type transforms are defined as maps between vector spaces, both of which have dim $q^N$,

$$V_A = \left\{ \left(h_{\underline{a}}\right)_A \mid \underline{a} \in A, \, h_{\underline{a}} \in \mathbb{F}_q \right\} ,$$
$$V_\Omega = \left\{ \left(c_{\underline{\omega}}\right)_\Omega \mid \underline{\omega} \in \Omega, \, c_{\underline{\omega}} \in \mathbb{F}_q \right\} .$$

*Definition 1: (Generalization of the multidimensional DFT over $\mathbb{F}_q$)* A linear map $\mathcal{F}$ is defined by

$$\mathcal{F} : V_\Omega \to V_A \quad \left[ \left(c_{\underline{\omega}}\right)_\Omega \mapsto \left( \sum_{\underline{\omega} \in \Omega} c_{\underline{\omega}} \underline{\omega}^{\underline{a}} \right)_A \right] , \tag{1}$$

where $\underline{\omega}^{\underline{a}} = \omega_1^{a_1} \cdots \omega_N^{a_N}$, and $\omega^a$ is considered as the substituted value $\omega^a = x^a|_{x=\omega}$, i.e., $\omega^a$ =1 for all $\omega \in \mathbb{F}_q$ if $a = 0$. The linear map $\mathcal{F} : V_\Omega \to V_A$ of (1) is called a generalized DFT on $\mathbb{F}_q^N$. □

Then, $\mathcal{F}$ is actually equal to the compound of ordinary DFTs in $N$ and lower dimensions.

*Example 1:* Assume $N = 1$. Note that, if $a \neq 0$ and $\omega = 0$, then $\omega^a = 0$ trivially holds. Thus, $(\widetilde{c}_a)_A = \mathcal{F}\left((c_\omega)_\Omega\right) \in V_A$ can be directly written as

$$\widetilde{c}_a = \begin{cases} \sum_{\omega \in \Omega} c_\omega \omega^a = \sum_{\omega \in \Omega, \, \omega \neq 0} c_\omega \omega^a & a \neq 0 \\ \sum_{\omega \in \Omega} c_\omega & a = 0. \end{cases}$$

Assume $N = 2$. Then, for each $(a_1, a_2) = (a, b) \in A$, $(\widetilde{c}_{ab})_A = \mathcal{F}\left((c_{\psi\omega})_\Omega\right) \in V_A$ can be directly written as

$$\widetilde{c}_{ab} = \begin{cases} \sum_{(\psi,\omega) \in \Omega} c_{\psi\omega} \psi^a \omega^b = \sum_{(\psi,\omega) \in \Omega, \, \psi\omega \neq 0} c_{\psi\omega} \psi^a \omega^b & ab \neq 0 \\ \sum_{(\psi,\omega) \in \Omega} c_{\psi\omega} \psi^a = \sum_{(\psi,\omega) \in \Omega, \, \psi \neq 0} c_{\psi\omega} \psi^a & a \neq 0, \, b = 0 \\ \sum_{(\psi,\omega) \in \Omega} c_{\psi\omega} \omega^b = \sum_{(\psi,\omega) \in \Omega, \, \omega \neq 0} c_{\psi\omega} \omega^b & a = 0, \, b \neq 0 \\ \sum_{(\psi,\omega) \in \Omega} c_{\psi\omega} & a = b = 0. \end{cases}$$

Assume $N = 3$. Then, for each $(a_1, a_2, a_3) = (a, b, c) \in A$, $\left(\widetilde{c}_{abc}\right)_A = \mathcal{F}\left(\left(c_{\phi\psi\omega}\right)_\Omega\right) \in V_A$ can be directly written as

$$\widetilde{c}_{abc} = \begin{cases} \sum_{(\phi,\psi,\omega)\in\Omega} c_{\phi\psi\omega}\phi^a\psi^b\omega^c = \sum_{(\phi,\psi,\omega)\in\Omega,\, \phi\psi\omega\neq 0} c_{\phi\psi\omega}\phi^a\psi^b\omega^c & abc \neq 0 \\ \sum_{(\phi,\psi,\omega)\in\Omega} c_{\phi\psi\omega}\phi^a\psi^b = \sum_{(\phi,\psi,\omega)\in\Omega,\, \phi\psi\neq 0} c_{\phi\psi\omega}\phi^a\psi^b & ab \neq 0,\ c = 0 \\ \sum_{(\phi,\psi,\omega)\in\Omega} c_{\phi\psi\omega}\phi^a\omega^c = \sum_{(\phi,\psi,\omega)\in\Omega,\, \phi\omega\neq 0} c_{\phi\psi\omega}\phi^a\omega^c & ac \neq 0,\ b = 0 \\ \sum_{(\phi,\psi,\omega)\in\Omega} c_{\phi\psi\omega}\psi^b\omega^c = \sum_{(\phi,\psi,\omega)\in\Omega,\, \psi\omega\neq 0} c_{\phi\psi\omega}\psi^b\omega^c & bc \neq 0,\ a = 0 \\ \sum_{(\phi,\psi,\omega)\in\Omega} c_{\phi\psi\omega}\phi^a = \sum_{(\phi,\psi,\omega)\in\Omega,\, \phi\neq 0} c_{\phi\psi\omega}\phi^a & a \neq 0,\ b = c = 0 \\ \sum_{(\phi,\psi,\omega)\in\Omega} c_{\phi\psi\omega}\psi^b = \sum_{(\phi,\psi,\omega)\in\Omega,\, \psi\neq 0} c_{\phi\psi\omega}\psi^b & b \neq 0,\ a = c = 0 \\ \sum_{(\phi,\psi,\omega)\in\Omega} c_{\phi\psi\omega}\omega^c = \sum_{(\phi,\psi,\omega)\in\Omega,\, \omega\neq 0} c_{\phi\psi\omega}\omega^c & c \neq 0,\ a = b = 0 \\ \sum_{(\phi,\psi,\omega)\in\Omega} c_{\phi\psi\omega} & a = b = c = 0. \end{cases}$$

In general, to write $\mathcal{F}$ directly requires $2^N$ equalities. □

*Definition 2: (Generalization of the multidimensional IDFT over* $\mathbb{F}_q$*)* For each $\underline{\omega} \in \Omega$, a subset $I = I_{\underline{\omega}} = \{i_1 \cdots, i_m\}$ of $[1, N]$ is determined such that $\omega_{i_1} \cdots \omega_{i_m} \neq 0$ and $\omega_i = 0$ for all $i \in [1, N] \setminus I$. A linear map $\mathcal{F}^{-1}$ is then defined by

$$\mathcal{F}^{-1} : V_A \to V_\Omega \quad \left[\left(h_{\underline{a}}\right)_A \mapsto \left(\widehat{h}_{\underline{\omega}}\right)_\Omega\right], \tag{2}$$

where

$$\widehat{h}_{\underline{\omega}} = (-1)^m \sum_{l_1,\cdots,l_m=1}^{q-1} \left\{ \sum_{J\subseteq[1,N]\setminus I} (-1)^{|J|} h_{\underline{i}(I,J)} \right\} \omega_{i_1}^{-l_1} \cdots \omega_{i_m}^{-l_m}, \tag{3}$$

$J$ in the sum runs over all subsets of $[1, N]\setminus I$, and $\underline{i}(I, J) = (b_1, \cdots, b_N) \in A$ is defined by, for $1 \leq i \leq N$,

$$b_i = \begin{cases} l_i & i \in I \\ q-1 & i \in J \\ 0 & i \in [1, N] \setminus (I \cup J)\ . \end{cases}$$

The linear map $\mathcal{F}^{-1} : V_A \to V_\Omega$ of (2) is called a generalized IDFT on $\mathbb{F}_q^N$. □

For example, if $\omega_1 \cdots \omega_N \neq 0$ for $\underline{\omega} = (\omega_1, \cdots, \omega_N) \in \Omega$, then $I$ is equal to $[1, N]$ and there is only one choice of $J = \emptyset$. In this case, definition (3) implies

$$\widehat{h}_{\underline{\omega}} = (-1)^N \sum_{l_1,\cdots,l_N=1}^{q-1} h_{(l_1,\cdots,l_N)} \omega_{i_1}^{-l_1} \cdots \omega_{i_N}^{-l_N},$$

in other words, $\mathcal{F}^{-1}$ agrees with the $N$-D IDFT if $\Omega$ is restricted to $\left(\mathbb{F}_q^\times\right)^N$. [1] In general, for each $\underline{\omega} \in \Omega$, the value $\widehat{h}_{\underline{\omega}}$ is equal to a linear combination of IDFTs whose dimensions do not exceed $N$.

[1] For this special case, including a motivating example of Reed–Solomon codes, see [22].

*Example 2:* Assume $N = 1$. If $\omega \neq 0 \in \Omega$, then $I = \{1\} \subseteq [1,1]$, $J = \emptyset \subseteq [1,1] \backslash I = \emptyset$, and $\underline{i}(I,J) = l_1 = i$. If $\omega = 0 \in \Omega$, then $I = \emptyset \subseteq [1,1]$, $J = \emptyset$ or $\{1\} \subseteq [1,1] \backslash I = \{1\}$, and $\underline{i}(I,J) = 0, q-1$, respectively. Thus, $\mathcal{F}^{-1}\left((h_a)_A\right) = \left(\widehat{h}_\omega\right)_\Omega \in V_\Omega$ can be directly written as

$$\widehat{h}_\omega = \begin{cases} -\sum_{i=1}^{q-1} h_i \omega^{-i} & \omega \neq 0 \\ h_0 - h_{q-1} & \omega = 0. \end{cases}$$

Assume $N = 2$. For $(\omega_1, \omega_2) = (\psi, \omega) \in \Omega$, e.g., if $\psi\omega \neq 0$, then $I = \{1,2\} \subseteq [1,2]$, $J = \emptyset \subseteq [1,2] \backslash I = \emptyset$, and $\underline{i}(I,J) = (l_1, l_2) = (i,j)$; if $\psi \neq 0$ and $\omega = 0$, then $I = \{1\} \subseteq [1,2]$, $J = \emptyset$ or $\{2\} \subseteq [1,2] \backslash I = \{2\}$, and $\underline{i}(I,J) = \underline{i}(\{1\}, J) = (i,0), (i, q-1)$, respectively. Thus, $\mathcal{F}^{-1}\left(\left(h_{\underline{a}}\right)_A\right) = \left(\widehat{h}_{\psi\omega}\right)_\Omega \in V_\Omega$ can be directly written as

$$\widehat{h}_{\psi\omega} = \begin{cases} \sum_{i,j=1}^{q-1} h_{ij} \psi^{-i} \omega^{-j} & \psi\omega \neq 0 \\ -\sum_{i=1}^{q-1} (h_{i,0} - h_{i,q-1}) \psi^{-i} & \psi \neq 0,\, \omega = 0 \\ -\sum_{j=1}^{q-1} (h_{0,j} - h_{q-1,j}) \omega^{-j} & \psi = 0,\, \omega \neq 0 \\ h_{0,0} - h_{0,q-1} - h_{q-1,0} + h_{q-1,q-1} & \psi = \omega = 0. \end{cases}$$

Assume $N = 3$. For $(\omega_1, \omega_2, \omega_3) = (\phi, \psi, \omega) \in \Omega$, e.g., if $\phi \neq 0$, $\psi = \omega = 0$, then $I = \{1\} \subseteq [1,3] = \{1,2,3\}$. Hence, $J \subseteq [1,3] \backslash I = \{2,3\}$ has four choices, i.e., $J = \emptyset, \{2\}, \{3\}, \{2,3\}$, and so, $\underline{i}(I,J) = \underline{i}(\{1\}, J) = (i,0,0), (i,q-1,0), (i,0,q-1), (i,q-1,q-1)$, respectively. Thus, $\mathcal{F}^{-1}\left(\left(h_{\underline{a}}\right)_A\right) = \left(\widehat{h}_{\phi\psi\omega}\right)_\Omega \in V_\Omega$ can be directly written as

$$\widehat{h}_{\phi\psi\omega} = \begin{cases} -\sum_{i,j,l=1}^{q-1} h_{ijl} \phi^{-i} \psi^{-j} \omega^{-l} & \phi\psi\omega \neq 0 \\ \sum_{i,j=1}^{q-1} (h_{i,j,0} - h_{i,j,q-1}) \phi^{-i} \psi^{-j} & \phi\psi \neq 0,\, \omega = 0 \\ \sum_{i,l=1}^{q-1} (h_{i,0,l} - h_{i,q-1,l}) \phi^{-i} \omega^{-l} & \phi\omega \neq 0,\, \psi = 0 \\ \sum_{j,l=1}^{q-1} (h_{0,j,l} - h_{q-1,j,l}) \psi^{-j} \omega^{-l} & \psi\omega \neq 0,\, \phi = 0 \\ -\sum_{i=1}^{q-1} (h_{i,0,0} - h_{i,q-1,0} - h_{i,0,q-1} + h_{i,q-1,q-1}) \phi^{-i} & \phi \neq 0,\, \psi = \omega = 0 \\ -\sum_{j=1}^{q-1} (h_{0,j,0} - h_{q-1,j,0} - h_{0,j,q-1} + h_{q-1,j,q-1}) \psi^{-j} & \psi \neq 0,\, \phi = \omega = 0 \\ -\sum_{l=1}^{q-1} (h_{0,0,l} - h_{q-1,0,l} - h_{0,q-1,l} + h_{q-1,q-1,l}) \omega^{-l} & \omega \neq 0,\, \phi = \psi = 0 \\ \begin{array}{l} h_{0,0,0} - h_{0,0,q-1} - h_{0,q-1,0} - h_{q-1,0,0} \\ \quad + h_{0,q-1,q-1} + h_{q-1,0,q-1} + h_{q-1,q-1,0} - h_{q-1,q-1,q-1} \end{array} & \phi = \psi = \omega = 0. \end{cases}$$

In general, the summand in each condition of $\underline{\omega}$ consists of $2^{N-m}$ terms, where $m$ is the number of non-zero components in $\underline{\omega}$. □

*Proposition 1: (Generalization of the Fourier inversion formulae)* Two linear maps $\mathcal{F} : V_\Omega \to V_A$ and $\mathcal{F}^{-1} : V_A \to V_\Omega$ are the inverse of each other, i.e., $\mathcal{F}^{-1}\left(\mathcal{F}\left(\left(c_{\underline{\omega}}\right)_\Omega\right)\right) = \left(c_{\underline{\omega}}\right)_\Omega$ and $\mathcal{F}\left(\mathcal{F}^{-1}\left(\left(h_{\underline{a}}\right)_A\right)\right) = \left(h_{\underline{a}}\right)_A$. $\square$
The proof is described in Appendix A. This proposition corresponds to one of the basic concepts in this paper.

## IV. Main Lemma

### A. *Two vector spaces $V_D$ and $V_\Psi$*

Let $\Psi \subseteq \Omega$ with $\Psi \neq \emptyset$ and $n = |\Psi|$. One of the two vector spaces in the lemma is given by

$$V_\Psi = \left\{ \left(c_{\underline{\psi}}\right)_\Psi \,\middle|\, \underline{\psi} \in \Psi,\, c_{\underline{\psi}} \in \mathbb{F}_q \right\},$$

namely, $V_\Psi$ is the vector space over $\mathbb{F}_q$ indexed by the elements of $\Psi$ whose dimension is trivially $n$. The other of the two vector spaces is somewhat complicated to define, as it requires Gröbner basis theory [6]. Let $\mathbb{F}_q[\underline{x}]$ be the ring of polynomials with coefficients in $\mathbb{F}_q$ whose variables are $x_1, \cdots, x_N$. Let $Z_\Psi$ be an ideal of $\mathbb{F}_q[\underline{x}]$ defined by

$$Z_\Psi = \left\{ f(\underline{x}) \in \mathbb{F}_q[\underline{x}] \mid f(\underline{\psi}) = 0 \text{ for all } \underline{\psi} \in \Psi \right\}.$$

Note that $x_i^q - x_i \in Z_\Psi$ for all $1 \leq i \leq N$, as $\Psi \neq \emptyset$. We fix a monomial order $\preceq$ of $\left\{ \underline{x}^{\underline{d}} \,\middle|\, \underline{d} \in \mathbb{N}_0^N \right\}$ [6], and then denote, for $f(\underline{x}) \in \mathbb{F}_q[\underline{x}]$,

$$\begin{aligned} &\mathrm{LM}(f) = \max_{\preceq} \left\{ \underline{x}^{\underline{d}} \,\middle|\, \underline{d} \in \mathbb{N}_0^N,\, f_{\underline{d}} \neq 0 \right\} \\ &\text{if } \ f(\underline{x}) = \sum_{\underline{d} \in \mathbb{N}_0^N,\, f_{\underline{d}} \neq 0} f_{\underline{d}} \underline{x}^{\underline{d}} \in \mathbb{F}_q[\underline{x}] \ \text{ and } f(\underline{x}) \neq 0, \end{aligned}$$

where $\underline{x}^{\underline{d}} = x_1^{d_1} \cdots x_N^{d_N}$ for $\underline{d} = (d_1, \cdots, d_N) \in \mathbb{N}_0^N$, and $\mathrm{LM}(f)$ is called the leading monomial of $f(\underline{x}) \in \mathbb{F}_q[\underline{x}]$. The delta set $D = D(\Psi) \subseteq \mathbb{N}_0^N$ of $Z_\Psi$ for $\Psi$ [29] is then defined by

$$D = D(\Psi) = \mathbb{N}_0^N \Big\backslash \left\{ \mathrm{mdeg}\left(\mathrm{LM}(f)\right) \mid 0 \neq f(\underline{x}) \in Z_\Psi \right\},$$

where $\mathrm{mdeg}\left(\underline{x}^{\underline{d}}\right) = \underline{d} \in \mathbb{N}_0^N$. Fortunately, $D(\Psi)$ has an intuitive description if a Gröbner basis $\mathcal{G}_\Psi$ of $Z_\Psi$ is obtained; it corresponds to the area surrounded by $\mathrm{LM}\left(\mathcal{G}_\Psi\right)$. The delta set $D = D(\Psi) \subseteq \mathbb{N}_0^N$ of $Z_\Psi$ for $\Psi$ is equivalently defined by

$$\begin{aligned} &\left\{ \underline{x}^{\underline{d}} \,\middle|\, \underline{d} \in D(\Psi) \right\} = \\ &\qquad \left\{ \underline{x}^{\underline{d}} \,\middle|\, \underline{d} \in \mathbb{N}_0^N \right\} \Big\backslash \left\{ \mathrm{LM}(f) \mid 0 \neq f(\underline{x}) \in Z_\Psi \right\}. \end{aligned}$$

The other of the two vector spaces is then given by

$$V_D = V_{D(\Psi)} = \left\{ \left(h_{\underline{d}}\right)_D \,\middle|\, \underline{d} \in D(\Psi),\, h_{\underline{d}} \in \mathbb{F}_q \right\},$$

namely, the vector space over $\mathbb{F}_q$ indexed by the elements of $D(\Psi)$. It is known [8] that the evaluation map

$$\mathrm{ev} : \mathbb{F}_q[\underline{x}]/Z_\Psi \to V_\Psi \quad \left[ f\left(\underline{x}\right) \mapsto \left( f\left(\underline{\psi}\right)\right)_\Psi \right] \tag{4}$$

is isomorphic. [2] Because $\left\{\underline{x}^{\underline{d}} \,\middle|\, \underline{d}\in D(\Psi)\right\}$ is a basis of the quotient ring $\mathbb{F}_q[\underline{x}]/Z_\Psi$ viewed as a vector space over $\mathbb{F}_q$, $\mathbb{F}_q[\underline{x}]/Z_\Psi$ is isomorphic to $V_D$. Thus, the map (4) can also be written as

$$\mathrm{ev}: V_D \to V_\Psi \quad \left[\left(h_{\underline{d}}\right)_D \mapsto \left(\sum_{\underline{d}\in D} h_{\underline{d}}\underline{\psi}^{\underline{d}}\right)_\Psi\right]. \tag{5}$$

In particular, it follows from the isomorphism (4) or (5) that $|D(\Psi)| = |\Psi|$ and $\dim_{\mathbb{F}_q} V_D = n$.

Because $V_D$ and $V_\Psi$ have the same dimension $n$, it is trivial that $V_D$ is isomorphic to $V_\Psi$ as a vector space over $\mathbb{F}_q$. However, this type of isomorphic maps depends on the choice of the bases of the vector spaces; additionally, in coding theory, the normal orthogonal basis is not always convenient for encoding and decoding. Our lemma asserts that there is a canonical isomorphic map that does not depend on the bases. As explained in Introduction, the isomorphic map $V_D \to V_\Psi$ of the lemma is given by the composition of the extension defined in the next subsection and the IDFT.

### B. Extension map $\mathcal{E}: V_D \to V_A$

Let $\mathcal{G}_\Psi$ be a Gröbner basis for the ideal $Z_\Psi$ with respect to $\preceq$. We assume that $\mathcal{G}_\Psi$ consists of $b$ elements $\{g^{(w)}\}_{0\le w<b}$, where

$$\begin{aligned} &g^{(w)} = g^{(w)}(\underline{x}) = \\ &\underline{x}^{\underline{d}_w} + \sum_{\underline{d}\in D(\Psi)} g^{(w)}_{\underline{d}}\underline{x}^{\underline{d}} \in Z_\Psi \ \text{ with } \underline{d}_w \in \mathbb{N}_0^N \setminus D(\Psi). \end{aligned} \tag{6}$$

From now on, $A = [0, q-1]^N$ is considered as a semigroup by the componentwise addition $\underline{a}+\underline{b}$ for $\underline{a} = (a_1, \cdots, a_N), \underline{b} = (b_1, \cdots, b_N) \in A$, where the component $a_i + b_i$ is viewed within $1 \le (a_i + b_i \bmod (q-1)) < q$ if $a_i + b_i \neq 0$ for $1 \le i \le N$. For example, $(0,0,1,2) + (0,3,1,2) = (0,3,2,1)$ in $A$ if $N=4$ and $q=4$. This semigroup structure of $A$ comes naturally from the multiplication of monomials in $\mathbb{F}_q[\underline{x}]/Z_\Omega$, which is isomorphic to $V_A$ as a vector space because $D(\Omega) = A$.

Furthermore, for $\underline{a}, \underline{b} \in A$, we denote $\underline{a} \ge \underline{b}$ if $a_i \ge b_i$ component-wise for all $1 \le i \le N$, or equivalently, if there is $\underline{c} \in A$ such that $\underline{a} = \underline{b} + \underline{c}$.

*Definition 3: (Map from multidimensional linear feedback shift registers)* A linear map $\mathcal{E}$ is defined by

$$\mathcal{E}: V_D \to V_A \quad \left[\left(h_{\underline{d}}\right)_D \mapsto \left(k_{\underline{a}}\right)_A\right], \tag{7}$$

where, for all $\underline{a} \in A$ and all $0 \le w < b$,

$$k_{\underline{a}} = \begin{cases} h_{\underline{d}} & \underline{a} = \underline{d} \in D(\Psi) \\ -\sum_{\underline{d}\in D(\Psi)} g^{(w)}_{\underline{d}} k_{\underline{a}+\underline{d}-\underline{d}_w} & \underline{a} \ge \underline{d}_w. \end{cases} \qquad \square \tag{8}$$

To actually compute the value of $\mathcal{E}\left(\left(h_{\underline{d}}\right)_D\right) = \left(k_{\underline{a}}\right)_A$ from a given $\left(h_{\underline{d}}\right)_D$, we generate $(k_{\underline{a}})_A$ inductively by (8), where, for each $\underline{a} \in A \backslash D(\Psi)$, at least one $0 \le w < b$ can be chosen such that $\underline{a} \ge \underline{d}_w$, and the resulting value

[2] The proof is quoted from [8]; the kernel of ev is trivially $Z_\Psi$ and the image of ev is $V_\Psi$ as, for $\underline{\phi} \in \Psi$, $f_{\underline{\phi}}(\underline{x}) = \prod_{i=1}^N \left\{1 - (x_i - \phi_i)^{q-1}\right\}$ satisfies $f_{\underline{\phi}}\left(\underline{\phi}\right) = 1$ and $f_{\underline{\phi}}\left(\underline{\psi}\right) = 0$ for all $\underline{\psi} \neq \underline{\phi}$.

does not depend on the choice and order of the generation. [3] Note that each $k_{\underline{a}}$ for $\underline{a} \in A \setminus D(\Psi)$ satisfies at least one recurrence relation, and in some case $b$ recurrence relations, from $\mathcal{G}_\Psi$.

*Proposition 2: (Prolongation via $\mathcal{E}$ for the linear sum of monomial values)* Let $\left(h_{\underline{d}}\right)_D \in V_D$. Suppose that there exists $\left(\epsilon_{\underline{\psi}}\right)_\Psi \in V_\Psi$ such that $\left(h_{\underline{d}}\right)_D = \left(\sum_{\underline{\psi}\in\Psi} \epsilon_{\underline{\psi}} \underline{\psi}^{\underline{d}}\right)_D$. Moreover, let $\left(k_{\underline{a}}\right)_A = \mathcal{E}\left(\left(h_{\underline{d}}\right)_D\right) \in V_A$. Then, it follows that $\left(k_{\underline{a}}\right)_A = \left(\sum_{\underline{\psi}\in\Psi} \epsilon_{\underline{\psi}} \underline{\psi}^{\underline{a}}\right)_A$. □

The proof of this proposition is described in Appendix B.

Consider a linear map $\mathcal{P}$ given by

$$\mathcal{P} : V_\Psi \to V_D \quad \left[\left(c_{\underline{\psi}}\right)_\Psi \mapsto \left(\sum_{\underline{\psi}\in\Psi} c_{\underline{\psi}} \underline{\psi}^{\underline{d}}\right)_D\right], \tag{9}$$

which is called a proper transform [29], and denote by $\mathcal{I}$ the inclusion map

$$\mathcal{I} : V_\Psi \to V_\Omega \quad \left[\left(c_{\underline{\psi}}\right)_\Psi \mapsto \left(c_{\underline{\omega}}\right)_\Omega\right],$$

where $c_{\underline{\omega}} = c_{\underline{\psi}}$ if $\underline{\omega} = \underline{\psi} \in \Psi$ and $c_{\underline{\omega}} = 0$ if $\underline{\omega} \notin \Psi$. Then, Proposition 2 asserts that the following commutative diagram, i.e., $\mathcal{E} \circ \mathcal{P} = \mathcal{F} \circ \mathcal{I}$, exists.

$$\begin{tikzcd}
V_A & V_\Omega \arrow[l, "\mathcal{F}"'] \\
V_D \arrow[u, "\mathcal{E}"] & V_\Psi \arrow[l, "\mathcal{P}"'] \arrow[u, "\mathcal{I}"']
\end{tikzcd} \tag{10}$$

*Proposition 3: (Relation between* ev *and $\mathcal{P}$)* If the normal orthogonal bases are taken as those of $V_D$ and $V_\Psi$, then the two matrices that represent $\mathrm{ev} : V_D \to V_\Psi$ in (5) and $\mathcal{P} : V_\Psi \to V_D$ in (9) are the transpose of each other. □

The proof is described in Appendix C. It follows from Proposition 3 that $\mathcal{P}$ is also isomorphic; this fact is noted in [29].

### C. Isomorphic map $\mathcal{C} : V_D \to V_\Psi$

From now on, we denote $\mathcal{R}$ as the restriction map

$$\mathcal{R} : V_\Omega \to V_\Psi \quad \left[\left(c_{\underline{\omega}}\right)_\Omega \mapsto \left(c_{\underline{\psi}}\right)_\Psi\right].$$

It follows from (10) that $\mathcal{F}^{-1} \circ \mathcal{E} \circ \mathcal{P} = \mathcal{I}$. Moreover, $\mathcal{R} \circ \mathcal{F}^{-1} \circ \mathcal{E} \circ \mathcal{P} = \mathcal{R} \circ \mathcal{I}$ is the identity map on $V_\Psi$. This leads to the following lemma, which is frequently used in this paper.

*Main Lemma :* Let $\mathcal{G}_\Psi$ be a Gröbner basis of $Z_\Psi$ for $\Psi \subseteq \Omega$, and let $\mathcal{E} : V_D \to V_A$ be the extension map defined by (7). Then, the composition map $\mathcal{C} = \mathcal{R} \circ \mathcal{F}^{-1} \circ \mathcal{E} : V_D \to V_\Psi$ in the following commutative diagram gives an

[3] If there are $\underline{a} \in A$ and $0 \leq v \neq w < b$ such that $\underline{a} \geq \underline{d}_v$ and $\underline{a} \geq \underline{d}_w$, then it follows from $\underline{x}^{\underline{a}-\underline{d}_v} g^{(v)} - \underline{x}^{\underline{a}-\underline{d}_w} g^{(w)} \in Z_\Psi$ that $\sum_{\underline{d}\in D(\Psi)} g_{\underline{d}}^{(v)} k_{\underline{a}+\underline{d}-\underline{d}_v} = \sum_{\underline{d}\in D(\Psi)} g_{\underline{d}}^{(w)} k_{\underline{a}+\underline{d}-\underline{d}_w}$. Thus, $k_{\underline{a}}$ does not depend on the choice and order of $v, w$.

isomorphism between $V_D$ and $V_\Psi$.

$$\begin{tikzcd}
V_A \arrow[r, "\mathcal{F}^{-1}"] & V_\Omega \arrow[d, "\mathcal{R}"] \\
V_D \arrow[u, "\mathcal{E}"] \arrow[r, "\mathcal{C}"] & V_\Psi
\end{tikzcd}$$

Moreover, we have that

$$\left(c_{\underline{\omega}}\right)_\Omega \in \mathcal{F}^{-1}\left(\mathcal{E}\left(V_D\right)\right) \implies c_{\underline{\omega}} = 0 \text{ for all } \underline{\omega} \in \Omega \backslash \Psi. \ \square \tag{11}$$

*Remark 1:* As $\mathcal{C} = \mathcal{P}^{-1}$, our $\mathcal{C}$ can also be obtained from the multiplication of the inverse matrix representing (9). However, if $\Psi$ is changed, then the inverse matrix must be computed each time. As $\Psi$ takes, e.g., the set of erasure-and-error locations and $\mathcal{C}$ has a lower computational complexity order than Gaussian elimination, there are many cases where $\mathcal{C}$ outperforms computing the inverse matrix, as shown in Section VI. □

*Remark 2:* The above proof of our Main Lemma can also be applied to the non-zero indexed case [19],[22] where $A = [0, q-2]^N$ has a cyclic structure mod $(q-1)$ and $\Omega = \left(\mathbb{F}_q^\times\right)^N$. □

*Example 3:* Putting $N = 1$, $q = 8$, and $\alpha \in \mathbb{F}_8$ with $\alpha^3+\alpha+1 = 0$, consider the natural order $\preceq$ to be a monomial order, i.e., $0 \preceq 1 \preceq 2 \preceq \cdots \preceq 7$ on $A = [0, 7]$. Choose $\Psi \subseteq \Omega = \{0, 1, \alpha, \alpha^2, \cdots, \alpha^6\}$ as $\Psi = \{0, \alpha, \alpha^3, \alpha^6\}$. Then, $D = D(\Psi) = \{0, 1, 2, 3\}$ and $\mathcal{G}_\Psi = \{g(x)\}$, where

$$g(x) = \prod_{\psi \in \Psi} (x - \psi) = \alpha^3 x + \alpha^3 x^2 + \alpha^2 x^3 + x^4.$$

For $(h_d)_D = (h_0, h_1, h_2, h_3) = (\alpha^2, \alpha^3, \alpha^5, 1)$, $\mathcal{E}\left((h_d)_D\right) = (h_a)_A = (h_0, h_1, \cdots, h_7)$ is given by

$$(h_4, h_5, h_6, h_7) = \left(\alpha^3, \alpha^4, \alpha^3, \alpha^3\right)$$

and $\mathcal{F}^{-1}\left(\mathcal{E}\left((h_d)_D\right)\right) = (c_\omega)_\Omega$ is given by

$$(c_0, c_1, c_\alpha, \cdots, c_{\alpha^6}) = \left(\alpha^5, 0, \alpha^2, 0, 1, 0, 0, \alpha^4\right).$$

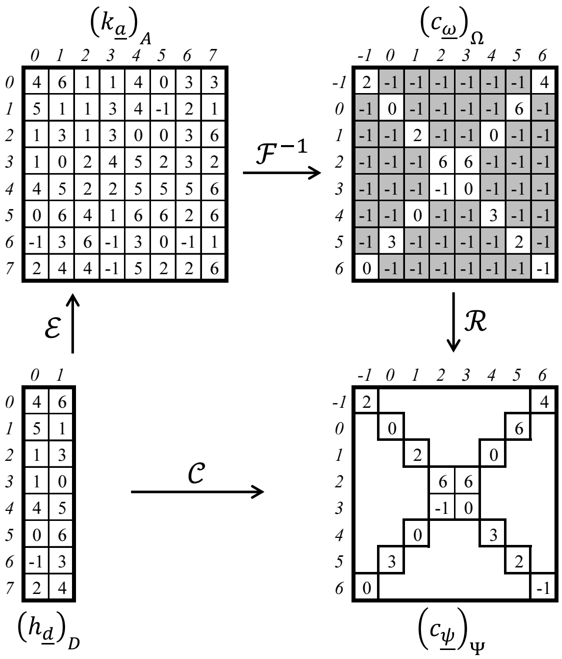
Note that $c_\omega = 0$ if $\omega \notin \Psi$. Then, $\mathcal{C}\left((h_d)_D\right) = (c_\psi)_\Psi = (c_0, c_\alpha, c_{\alpha^3}, c_{\alpha^6}) = \left(\alpha^5, \alpha^2, 1, \alpha^4\right)$. □

*Example 4:* Putting $N = 2$, $q = 8$, and $\alpha \in \mathbb{F}_8$ with $\alpha^3 + \alpha + 1 = 0$, consider the lexicographic order $\preceq$ to be a monomial order, i.e., $(0, 0) \preceq (1, 0) \preceq (2, 0) \preceq \cdots \preceq (7, 0) \preceq (0, 1) \preceq (1, 1) \preceq \cdots \preceq (7, 7)$ on $A = [0, 7]^2$. Choose $\Psi \subseteq \Omega = \mathbb{F}_8^2$ as

$$\Psi = \left\{ \begin{array}{l} (0,0), (0,\alpha^6), (\alpha^0,\alpha^0), (\alpha^0,\alpha^5), \\ (\alpha^1,\alpha^1), (\alpha^1,\alpha^4), (\alpha^2,\alpha^2), (\alpha^2,\alpha^3), \\ (\alpha^3,\alpha^2), (\alpha^3,\alpha^3), (\alpha^4,\alpha^1), (\alpha^4,\alpha^4), \\ (\alpha^5,\alpha^0), (\alpha^5,\alpha^5), (\alpha^6,0), (\alpha^6,\alpha^6) \end{array} \right\}, \tag{12}$$

which, in order to show a pictorial example, is the cross pattern $\left(c_{\underline{\omega}}\right)_\Omega$ in Fig. 1. An element $g(x, y) \in \mathcal{G}_\Psi$ of the Gröbner basis can then be characterized as $g(x, y) \in \mathbb{F}_8[x, y]$ with $g(\psi, \omega) = 0$ for all $(\psi, \omega) \in \Psi$ that has the minimum $\mathrm{LM}(g)$ with respect to $\preceq$. One of $\mathcal{G}_\Psi$ is computed as

$$g(x, y) = \alpha^6 x + \alpha^0 x^2 + \alpha^1 x^3 + \alpha^2 x^4 + \alpha^3 x^5 + \alpha^4 x^6$$



$\left(k_{\underline{a}}\right)_A$

| | *0* | *1* | *2* | *3* | *4* | *5* | *6* | *7* |
|---|---|---|---|---|---|---|---|---|
| *0* | 4 | 6 | 1 | 1 | 4 | 0 | 3 | 3 |
| *1* | 5 | 1 | 1 | 3 | 4 | -1 | 2 | 1 |
| *2* | 1 | 3 | 1 | 3 | 0 | 0 | 3 | 6 |
| *3* | 1 | 0 | 2 | 4 | 5 | 2 | 3 | 2 |
| *4* | 4 | 5 | 2 | 2 | 5 | 5 | 5 | 6 |
| *5* | 0 | 6 | 4 | 1 | 6 | 6 | 2 | 6 |
| *6* | -1 | 3 | 6 | -1 | 3 | 0 | -1 | 1 |
| *7* | 2 | 4 | 4 | -1 | 5 | 2 | 2 | 6 |

$\left(c_{\underline{\omega}}\right)_\Omega$

| | *-1* | *0* | *1* | *2* | *3* | *4* | *5* | *6* |
|---|---|---|---|---|---|---|---|---|
| *-1* | 2 | -1 | -1 | -1 | -1 | -1 | -1 | 4 |
| *0* | -1 | 0 | -1 | -1 | -1 | -1 | 6 | -1 |
| *1* | -1 | -1 | 2 | -1 | -1 | 0 | -1 | -1 |
| *2* | -1 | -1 | -1 | 6 | 6 | -1 | -1 | -1 |
| *3* | -1 | -1 | -1 | -1 | 0 | -1 | -1 | -1 |
| *4* | -1 | -1 | 0 | -1 | -1 | 3 | -1 | -1 |
| *5* | -1 | 3 | -1 | -1 | -1 | -1 | 2 | -1 |
| *6* | 0 | -1 | -1 | -1 | -1 | -1 | -1 | -1 |

$\left(h_{\underline{d}}\right)_D$

| | *0* | *1* |
|---|---|---|
| *0* | 4 | 6 |
| *1* | 5 | 1 |
| *2* | 1 | 3 |
| *3* | 1 | 0 |
| *4* | 4 | 5 |
| *5* | 0 | 6 |
| *6* | -1 | 3 |
| *7* | 2 | 4 |

$\left(c_{\underline{\psi}}\right)_\Psi$

| | *-1* | *0* | *1* | *2* | *3* | *4* | *5* | *6* |
|---|---|---|---|---|---|---|---|---|
| *-1* | 2 | | | | | | | 4 |
| *0* | | 0 | | | | | 6 | |
| *1* | | | 2 | | | 0 | | |
| *2* | | | | 6 | 6 | | | |
| *3* | | | | -1 | 0 | | | |
| *4* | | | 0 | | | 3 | | |
| *5* | | 3 | | | | | 2 | |
| *6* | 0 | | | | | | | -1 |

Fig. 1. Numerical example of Main Lemma, where $\Psi$ is given by (12) in Example 4. The non-zero elements of $\mathbb{F}_8$ are represented by the number of powers of a primitive element $\alpha$ with $\alpha^3+\alpha+1=0$, i.e., $0,1,\cdots,6$ means $\alpha^0,\alpha^1,\cdots,\alpha^6$, respectively, and $-1$ means $0\in\mathbb{F}_8$. The value of $\left(c_{\underline{\omega}}\right)_\Omega$ in the shaded box indicates $c_{\underline{\omega}}$ on $\Omega$ outside the $\Psi$ of (12). Note that these values are all $-1$ according to assertion (11) of Main Lemma.

$$+\,y\left(\alpha^6+\alpha^1x^2+\alpha^2x^3+\alpha^3x^4+\alpha^4x^5\right)+y^2.$$

The other elements of $\mathcal{G}_\Psi$ are not necessary to extend $\left(h_{\underline{d}}\right)_D$ because of the semigroup structure of $A$; e.g., $k_{\underline{a}}$ with $\underline{a}=(8,0)$ can be regarded as $\alpha^5$. For a given $\left(h_{\underline{d}}\right)_D$, all values of Main Lemma are shown in Fig. 1, where the vertical axis and the horizontal axis (*0,1,$\cdots$,7*) in $\left(k_{\underline{a}}\right)_A$ indicate $a$ and $b$ of $\underline{a}=(a,b)\in A$, and those axes (*-1,0,$\cdots$,6*) in $\left(c_{\underline{\omega}}\right)_\Omega$ indicate $\psi$ and $\omega$ of $\underline{\omega}=(\psi,\omega)\in\Omega$. □

## V. Applications of Main Lemma

### *A. Affine variety codes [8]*

Let $\Psi\subseteq\Omega$ with $\Psi\neq\emptyset$ and $n=|\Psi|$, as at the beginning of Subsection IV-A. Let $U$ be a subspace of $V_{D(\Psi)}$. Consider an affine variety code [8] with code length $n$

$$\begin{aligned} C(U,\Psi) &= \mathrm{ev}(U) \qquad (13)\\ &= \left\{ \left(c_{\underline{\psi}}\right)_\Psi \in V_\Psi \;\middle|\; \begin{array}{l} \left(\sum_{\underline{d}\in D} h_{\underline{d}}\underline{\psi}^{\underline{d}}\right)_\Psi = \left(c_{\underline{\psi}}\right)_\Psi \\ \text{for some } \left(h_{\underline{d}}\right)_D \in U \end{array} \right\}, \end{aligned}$$

where $\underline{\psi}^{\underline{d}} = \psi_1^{d_1} \cdots \psi_N^{d_N}$ is as in (1). Moreover, consider a dual affine variety code [8] with code length $n$

$$\begin{aligned} C^{\perp}(U, \Psi) &= \mathrm{ev}(U)^{\perp} \qquad (14) \\ &= \left\{ \left(c_{\underline{\psi}}\right)_{\Psi} \in V_{\Psi} \;\middle|\; \begin{array}{l} \sum_{\underline{\psi} \in \Psi} c_{\underline{\psi}} \sum_{\underline{d} \in D} h_{\underline{d}} \underline{\psi}^{\underline{d}} = 0 \\ \text{for all } \left(h_{\underline{d}}\right)_D \in U \end{array} \right\}, \end{aligned}$$

where $\sum_{\underline{\psi} \in \Psi} c_{\underline{\psi}} \sum_{\underline{d} \in D} h_{\underline{d}} \underline{\psi}^{\underline{d}}$ in (14) is equal to the inner product of $\left(c_{\underline{\psi}}\right)_{\Psi}$ and $\mathrm{ev}\left(\left(h_{\underline{d}}\right)_D\right) = \left(\sum_{\underline{d} \in D} h_{\underline{d}} \underline{\psi}^{\underline{d}}\right)_{\Psi}$ in $V_{\Psi}$. Thus, the dimension or number of information symbols $k$ of $C^{\perp}(U, \Psi)$ is equal to $n - \dim_{\mathbb{F}_q} U$; in other words, $n - k = \dim_{\mathbb{F}_q} U$. Note that, as vector spaces, these code definitions do not depend on the choice of monomial order; $U \subseteq V_{D(\Psi)}$ is equivalent to $U \subseteq \mathbb{F}_q[\underline{x}]/Z_{\Psi}$.

On the other hand, let $U^{\perp}$ be the orthogonal complement of $U$ in $V_D$, i.e.,

$$U^{\perp} = \left\{ \left(h_{\underline{d}}\right)_D \in V_D \;\middle|\; \sum_{\underline{d} \in D} h_{\underline{d}} k_{\underline{d}} = 0 \text{ for all } \left(k_{\underline{d}}\right)_D \in U \right\}.$$

Then, similarly to (13), we obtain

$$C^{\perp}(U, \Psi) = \mathcal{C}\left(U^{\perp}\right), \qquad (15)$$

a proof of which is given in Appendix D. Whereas the definition (14) of $C^{\perp}(U, \Psi)$ is indirect and not constructive, the equality (15) provides a direct construction. Moreover, the equality (15) corresponds to the non-systematic encoding of $C^{\perp}(U, \Psi)$. Actually, non-systematic encoding is obtained, for all $\left(h_{\underline{d}}\right)_D \in U^{\perp}$, by $\left(c_{\underline{\psi}}\right)_{\Psi} = \mathcal{C}\left(\left(h_{\underline{d}}\right)_D\right) \in C^{\perp}(U, \Psi)$ as (15).

*Example 5:* (Continued from Example 3) Let $U \subseteq V_D$ be a vector space generated by $\left(1, 0, \alpha^4, \alpha^5\right)$ and $\left(0, 1, 0, \alpha^6\right)$. If these are represented as polynomials $f(x) = 1 + \alpha^4 x^2 + \alpha^5 x^3$ and $x + \alpha^6 x^3$, then $\mathrm{ev}(U) \subseteq V_{\Psi}$ is generated by

$$\begin{aligned} &\left(f(0), f(\alpha), f(\alpha^3), f(\alpha^6)\right) \\ &= \left(1, \alpha^4, \alpha^3, 1\right) \text{ and } \left(0, \alpha^4, 1, \alpha^4\right). \end{aligned}$$

Then, $U^{\perp} \subseteq V_D$ is equal to a vector space generated by

$$(u_0, u_1, u_2, u_3) = \left(\alpha^4, 0, 1, 0\right) \text{ and } \left(\alpha^5, \alpha^6, 0, 1\right).$$

These extensions are equal to

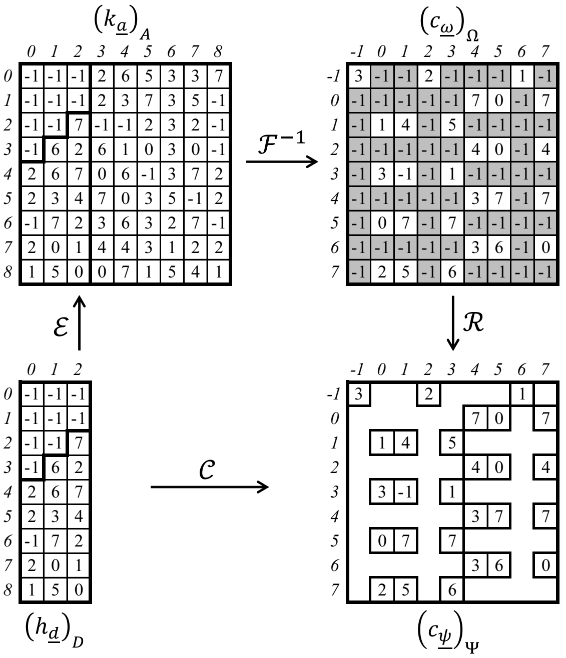
$$(u_4, u_5, u_6, u_7) = \left(\alpha^3, \alpha^2, \alpha^3, \alpha^6\right) \text{ and } \left(0, \alpha^3, \alpha^2, \alpha^3\right).$$

Thus, $\mathcal{C}\left(U^{\perp}\right)$ is generated by

$$(c_0, c_{\alpha}, c_{\alpha^3}, c_{\alpha^6}) = \left(\alpha^3, \alpha^5, \alpha^5, \alpha^6\right) \text{ and } \left(\alpha^2, \alpha^4, \alpha^2, 1\right).$$

The orthogonality is valid, e.g., $\alpha^3 + \alpha^2 + \alpha + \alpha^6 = 0$. □

*Remark 3:* A typical case of $U$ is $U = V_R$ for some $R \subseteq D(\Psi)$. Then, $U^{\perp} = V_{D \setminus R}$, where $V_R$ and $V_{D \setminus R}$ are considered subspaces of $V_D$, as in Section II. □



$\left(k_{\underline{a}}\right)_A$

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|---|
| 0 | -1 | -1 | -1 | 2 | 6 | 5 | 3 | 3 | 7 |
| 1 | -1 | -1 | -1 | 2 | 3 | 7 | 3 | 5 | -1 |
| 2 | -1 | -1 | 7 | -1 | -1 | 2 | 3 | 2 | -1 |
| 3 | -1 | 6 | 2 | 6 | 1 | 0 | 3 | 0 | -1 |
| 4 | 2 | 6 | 7 | 0 | 6 | -1 | 3 | 7 | 2 |
| 5 | 2 | 3 | 4 | 7 | 0 | 3 | 5 | -1 | 2 |
| 6 | -1 | 7 | 2 | 3 | 6 | 3 | 2 | 7 | -1 |
| 7 | 2 | 0 | 1 | 4 | 4 | 3 | 1 | 2 | 2 |
| 8 | 1 | 5 | 0 | 0 | 7 | 1 | 5 | 4 | 1 |

$\left(c_{\underline{\omega}}\right)_\Omega$

| | -1 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|---|
| -1 | 3 | -1 | -1 | 2 | -1 | -1 | -1 | 1 | -1 |
| 0 | -1 | -1 | -1 | -1 | -1 | 7 | 0 | -1 | 7 |
| 1 | -1 | 1 | 4 | -1 | 5 | -1 | -1 | -1 | -1 |
| 2 | -1 | -1 | -1 | -1 | -1 | 4 | 0 | -1 | 4 |
| 3 | -1 | 3 | -1 | -1 | 1 | -1 | -1 | -1 | -1 |
| 4 | -1 | -1 | -1 | -1 | -1 | 3 | 7 | -1 | 7 |
| 5 | -1 | 0 | 7 | -1 | 7 | -1 | -1 | -1 | -1 |
| 6 | -1 | -1 | -1 | -1 | -1 | 3 | 6 | -1 | 0 |
| 7 | -1 | 2 | 5 | -1 | 6 | -1 | -1 | -1 | -1 |

| | 0 | 1 | 2 |
|---|---|---|---|
| 0 | -1 | -1 | -1 |
| 1 | -1 | -1 | -1 |
| 2 | -1 | -1 | 7 |
| 3 | -1 | 6 | 2 |
| 4 | 2 | 6 | 7 |
| 5 | 2 | 3 | 4 |
| 6 | -1 | 7 | 2 |
| 7 | 2 | 0 | 1 |
| 8 | 1 | 5 | 0 |

$\left(h_{\underline{d}}\right)_D$

| | -1 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|---|
| -1 | 3 | | | 2 | | | | 1 | |
| 0 | | | | | | 7 | 0 | | 7 |
| 1 | | 1 | 4 | | 5 | | | | |
| 2 | | | | | | 4 | 0 | | 4 |
| 3 | | 3 | -1 | | 1 | | | | |
| 4 | | | | | | 3 | 7 | | 7 |
| 5 | | 0 | 7 | | 7 | | | | |
| 6 | | | | | | 3 | 6 | | 0 |
| 7 | | 2 | 5 | | 6 | | | | |

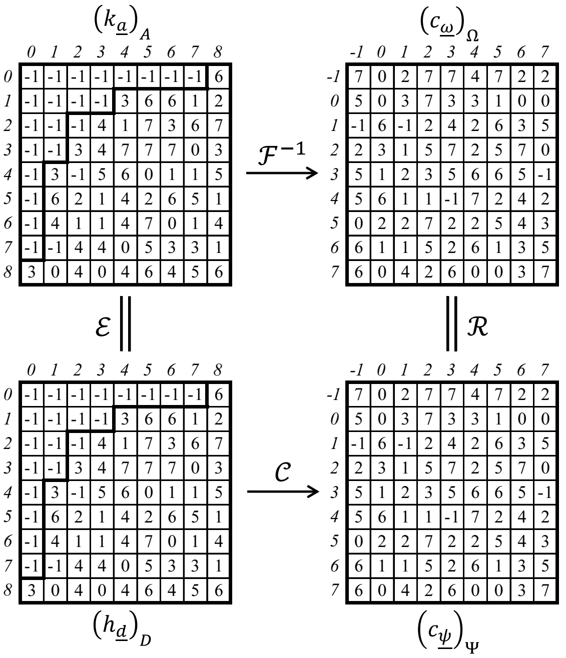
$\left(c_{\underline{\psi}}\right)_\Psi$

Fig. 2. Numerical example of the non-systematic encoding of a Hermitian code over $\mathbb{F}_9$ in Example 6. The non-zero elements of $\mathbb{F}_9$ are represented by the number of powers of a primitive element $\alpha$ with $\alpha^2+\alpha=1$, i.e., $0,1,\cdots,7$ means $\alpha^0,\alpha^1,\cdots,\alpha^7$, respectively, and $-1$ means $0\in\mathbb{F}_9$. The value of $\left(c_{\underline{\omega}}\right)_\Omega$ not in the shaded box indicates $c_{\underline{\omega}}$ on the $\Psi$ given by (16), and $\left(c_{\underline{\psi}}\right)_\Psi$ is a codeword of a Hermitian code.

*Example 6:* Throughout the rest of Section V, we consider a Hermitian code, i.e., a code on the $\mathbb{F}_9$-rational points of a Hermitian curve, in order to compare our method with conventional methods for algebraic geometry codes. Putting $N=2$, $q=9$, and $\alpha\in\mathbb{F}_9$ with $\alpha^2+\alpha-1=0$, consider the weighted graded lexicographic order [6] to be a monomial order $\preceq$ such that $(a,b)\preceq(a',b')\Leftrightarrow 3a+4b<3a'+4b'$ or $3a+4b=3a'+4b'$, $a\leq a'$, i.e., $(0,0)\preceq(1,0)\preceq(0,1)\preceq(2,0)\preceq(1,1)\preceq(0,2)\preceq\cdots\preceq(1,2)\preceq(4,0)\preceq(0,3)\preceq(3,1)\preceq\cdots\preceq(8,8)$ on $A=[0,8]^2$. Choose $\Psi\subseteq\Omega=\mathbb{F}_9^2$ as

$$\Psi=\left\{\begin{array}{l}(0,0),(0,\alpha^2),(0,\alpha^6),(\alpha^0,\alpha^4),\\ (\alpha^0,\alpha^5),(\alpha^0,\alpha^7),(\alpha^1,\alpha^0),(\alpha^1,\alpha^1),\\ (\alpha^1,\alpha^3),(\alpha^2,\alpha^4),(\alpha^2,\alpha^5),(\alpha^2,\alpha^7),\\ (\alpha^3,\alpha^0),(\alpha^3,\alpha^1),(\alpha^3,\alpha^3),(\alpha^4,\alpha^4),\\ (\alpha^4,\alpha^5),(\alpha^4,\alpha^7),(\alpha^5,\alpha^0),(\alpha^5,\alpha^1),\\ (\alpha^5,\alpha^3),(\alpha^6,\alpha^4),(\alpha^6,\alpha^5),(\alpha^6,\alpha^7),\\ (\alpha^7,\alpha^0),(\alpha^7,\alpha^1),(\alpha^7,\alpha^3),\end{array}\right\}, \quad (16)$$

which agrees with $\left\{(\psi,\omega)\in\mathbb{F}_9\,|\,\psi^4=\omega^3+\omega\right\}$, a set of $\mathbb{F}_9$-rational points of a Hermitian curve with defining equation $x^4=y^3+y$. In this case, one of the elements in the Gröbner basis $\mathcal{G}_\Psi$ is equal to $g(x,y)=x^4-y^3-y$ and the delta set $D(\Psi)$ of $\mathcal{G}_\Psi$ is $\{(a,b)\in A|\,b\leq 2\}$. The other elements of $\mathcal{G}_\Psi$ are not necessary to extend $\left(h_{\underline{d}}\right)_D$



$\left(k_{\underline{a}}\right)_A$

|  | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|---|
| 0 | -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 | 6 |
| 1 | -1 | -1 | -1 | -1 | 3 | 6 | 6 | 1 | 2 |
| 2 | -1 | -1 | -1 | 4 | 1 | 7 | 3 | 6 | 7 |
| 3 | -1 | -1 | 3 | 4 | 7 | 7 | 7 | 0 | 3 |
| 4 | -1 | 3 | -1 | 5 | 6 | 0 | 1 | 1 | 5 |
| 5 | -1 | 6 | 2 | 1 | 4 | 2 | 6 | 5 | 1 |
| 6 | -1 | 4 | 1 | 1 | 4 | 7 | 0 | 1 | 4 |
| 7 | -1 | -1 | 4 | 4 | 0 | 5 | 3 | 3 | 1 |
| 8 | 3 | 0 | 4 | 0 | 4 | 6 | 4 | 5 | 6 |

$\left(c_{\underline{\omega}}\right)_\Omega$

|  | -1 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|---|
| -1 | 7 | 0 | 2 | 7 | 7 | 4 | 7 | 2 | 2 |
| 0 | 5 | 0 | 3 | 7 | 3 | 3 | 1 | 0 | 0 |
| 1 | -1 | 6 | -1 | 2 | 4 | 2 | 6 | 3 | 5 |
| 2 | 2 | 3 | 1 | 5 | 7 | 2 | 5 | 7 | 0 |
| 3 | 5 | 1 | 2 | 3 | 5 | 6 | 6 | 5 | -1 |
| 4 | 5 | 6 | 1 | 1 | -1 | 7 | 2 | 4 | 2 |
| 5 | 0 | 2 | 2 | 7 | 2 | 2 | 5 | 4 | 3 |
| 6 | 6 | 1 | 1 | 5 | 2 | 6 | 1 | 3 | 5 |
| 7 | 6 | 0 | 4 | 2 | 6 | 0 | 0 | 3 | 7 |

|  | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|---|
| 0 | -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 | 6 |
| 1 | -1 | -1 | -1 | -1 | 3 | 6 | 6 | 1 | 2 |
| 2 | -1 | -1 | -1 | 4 | 1 | 7 | 3 | 6 | 7 |
| 3 | -1 | -1 | 3 | 4 | 7 | 7 | 7 | 0 | 3 |
| 4 | -1 | 3 | -1 | 5 | 6 | 0 | 1 | 1 | 5 |
| 5 | -1 | 6 | 2 | 1 | 4 | 2 | 6 | 5 | 1 |
| 6 | -1 | 4 | 1 | 1 | 4 | 7 | 0 | 1 | 4 |
| 7 | -1 | -1 | 4 | 4 | 0 | 5 | 3 | 3 | 1 |
| 8 | 3 | 0 | 4 | 0 | 4 | 6 | 4 | 5 | 6 |

$\left(h_{\underline{d}}\right)_D$

|  | -1 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|---|
| -1 | 7 | 0 | 2 | 7 | 7 | 4 | 7 | 2 | 2 |
| 0 | 5 | 0 | 3 | 7 | 3 | 3 | 1 | 0 | 0 |
| 1 | -1 | 6 | -1 | 2 | 4 | 2 | 6 | 3 | 5 |
| 2 | 2 | 3 | 1 | 5 | 7 | 2 | 5 | 7 | 0 |
| 3 | 5 | 1 | 2 | 3 | 5 | 6 | 6 | 5 | -1 |
| 4 | 5 | 6 | 1 | 1 | -1 | 7 | 2 | 4 | 2 |
| 5 | 0 | 2 | 2 | 7 | 2 | 2 | 5 | 4 | 3 |
| 6 | 6 | 1 | 1 | 5 | 2 | 6 | 1 | 3 | 5 |
| 7 | 6 | 0 | 4 | 2 | 6 | 0 | 0 | 3 | 7 |

$\left(c_{\underline{\psi}}\right)_\Psi$

Fig. 3. Numerical example for the non-systematic encoding of an extended HCRS code over $\mathbb{F}_9$ in Example 7. The elements of $\mathbb{F}_9$ are represented as in Fig. 2. Because $A = D$ and $\Omega = \Psi$ in this case, $\mathcal{E}$ and $\mathcal{R}$ are identity maps. $\left(c_{\underline{\psi}}\right)_\Psi$ is a codeword of an extended HCRS code.

because of the semigroup structure of $A$. Let $R \subseteq D(\Psi)$ be $R = \{\,(r_1, r_2) \in D(\Psi) |\, 3r_1 + 4r_2 \leq 11\}$ and let $U = V_R$. Then, $C^\perp(U, \Psi) = \mathcal{C}\left(V_{D(\Psi)\setminus R}\right)$ agrees with $C_\Omega(D, mP_\infty) = C_L(D, mP_\infty)^\perp$ in the usual notation [33] for $m = 11$ and $D = \sum_{(\psi,\omega)\in\Psi} P_{\psi,\omega}$ with $P_{\psi,\omega} = (\psi, \omega)$. For a given $\left(h_{\underline{d}}\right)_D$, all values of Main Lemma are shown in Fig. 2, where the vertical axis and the horizontal axis (*0,1,$\cdots$,8*) in $\left(k_{\underline{a}}\right)_A$ indicate $a$ and $b$ of $\underline{a} = (a, b) \in A$, and those axes (*-1,0,$\cdots$,7*) in $\left(c_{\underline{\omega}}\right)_\Omega$ indicate $\psi$ and $\omega$ of $\underline{\omega} = (\psi, \omega) \in \Omega$. □

*Example 7:* Throughout the rest of Section V, we consider an extended hyperbolic cascaded Reed–Solomon (HCRS) code, which is an example of affine variety codes that are not algebraic geometry codes. Putting $N = 2$, $q = 9$, and $\alpha \in \mathbb{F}_9$ with $\alpha^2 + \alpha - 1 = 0$, choose $\Psi = \Omega = \mathbb{F}_9^2$ and $A = [0, 8]^2$; then, $D = D(\Psi) = A$. Let $R \subseteq D(\Psi)$ be $R = \{\,(r_1, r_2) \in A |\, (r_1 + 1)(r_2 + 1) < 9\}$, and let $U = V_R$. Then, $C^\perp(U, \Omega) = \mathcal{C}\left(V_{A\setminus R}\right)$ is an extended HCRS code [9],[13],[28],[29]. For a given $\left(h_{\underline{d}}\right)_D$, all values of Main Lemma are shown in Fig. 3. □

In Subsection V-D, it is shown that Main Lemma also gives the systematic encoding of a class of dual affine variety codes.

### B. Erasure-and-error decoding: non-systematic case

Henceforth, consider the situation $U = V_R$ with some $R \subseteq D(\Psi)$ from Remark 3. In this subsection, suppose that $\left(h_{\underline{d}}\right)_D \in V_{D\setminus R}$ is encoded into $\left(c_{\underline{\psi}}\right)_\Psi = \mathcal{C}\left(\left(h_{\underline{d}}\right)_D\right) \in C^\perp(V_R, \Psi)$, and consider the decoding problem for this non-systematic encoding.

Suppose also that erasure-and-error $\left(e_{\underline{\psi}}\right)_{\Psi}$ has occurred in a received word $\left(u_{\underline{\psi}}\right)_{\Psi} = \left(c_{\underline{\psi}}\right)_{\Psi} + \left(e_{\underline{\psi}}\right)_{\Psi}$ from some channel. Let $\Phi_1 \subseteq \Psi$ be the set of erasure locations and $\Phi_2 \subseteq \Psi$ be the set of error locations with $\Phi_1 \cap \Phi_2 = \emptyset$; we suppose that $\Phi_1$ is known, but $\Phi_2$ and $\left(e_{\underline{\psi}}\right)_{\Psi}$ are unknown, that $e_{\underline{\psi}} \neq 0 \Rightarrow \underline{\psi} \in \Phi_1 \cup \Phi_2$, and that $\underline{\psi} \in \Phi_2 \Rightarrow e_{\underline{\psi}} \neq 0$. We might permit $e_{\underline{\psi}} = 0$ for some $\underline{\psi} \in \Phi_1$. If $|\Phi_1| + 2|\Phi_2| < d_{\mathrm{FR}}$ is valid, where $d_{\mathrm{FR}}$ denotes the Feng–Rao minimum distance bound [1],[7],[23],[32], then it is known that the erasure-and-error version [14],[31] of the BMS algorithm [4],[7] or the multidimensional Berlekamp–Massey algorithm calculates the Gröbner basis $\mathcal{G}_{\Phi_1 \cup \Phi_2}$. The main difference between the erasure-and-error and ordinary error-only algorithms is in the initialization; as $\Phi_1$ is known, $\mathcal{G}_{\Phi_1}$ can be calculated in advance by the ordinary error-only version, and then $\mathcal{G}_{\Phi_1 \cup \Phi_2}$ can be calculated by the erasure-and-error version from the syndrome and the initial value $\mathcal{G}_{\Phi_1}$. Using the recurrence from $\mathcal{G}_{\Phi_1 \cup \Phi_2}$ and Main Lemma, the erasure-and-error decoding algorithm is realized as follows.

*Algorithm 1: (Decoding of non-systematic codewords)*

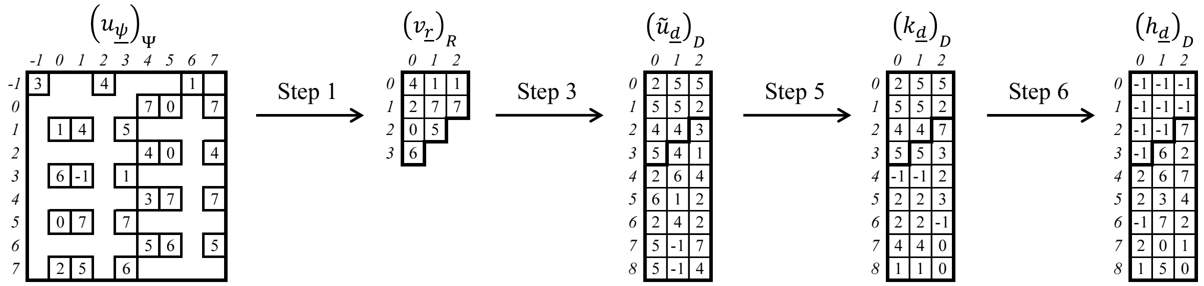
```
Input: $\Phi_1$ and a received word $\left(u_{\underline{\psi}}\right)_{\Psi} \in V_{\Psi}$
Output: $\left(h_{\underline{d}}\right)_D \in V_{D \setminus R}$ such that $\mathcal{C}\left(\left(h_{\underline{d}}\right)_D\right) = \left(c_{\underline{\psi}}\right)_{\Psi}$
Step 1. $\left(v_{\underline{r}}\right)_R = \left(\sum_{\underline{\psi} \in \Phi_1} \underline{\psi}^{\underline{r}}\right)_R \in V_R$
Step 2. Calculate $\mathcal{G}_{\Phi_1}$ from syndrome $\left(v_{\underline{r}}\right)_R$
Step 3. $\left(\widetilde{u}_{\underline{d}}\right)_D = \left(\sum_{\underline{\psi} \in \Psi} u_{\underline{\psi}} \underline{\psi}^{\underline{d}}\right)_D$
Step 4. Calculate $\mathcal{G}_{\Phi_1 \cup \Phi_2}$ from $\left(\widetilde{u}_{\underline{r}}\right)_R$ and $\mathcal{G}_{\Phi_1}$
Step 5. $\left(k_{\underline{d}}\right)_D = \mathcal{E}\left(\left(\widetilde{u}_{\underline{r}}\right)_R\right)$ by $\mathcal{G}_{\Phi_1 \cup \Phi_2}$
Step 6. $\left(h_{\underline{d}}\right)_D = \left(\widetilde{u}_{\underline{d}}\right)_D - \left(k_{\underline{d}}\right)_D$ □
```

At Step 5, $\left(k_{\underline{d}}\right)_D = \mathcal{E}\left(\left(\widetilde{u}_{\underline{r}}\right)_R\right)$ means that $\left(k_{\underline{d}}\right)_{D(\Psi)} = \mathcal{E}\left(\left(\widetilde{u}_{\underline{d}}\right)_{D(\Phi_1 \cup \Phi_2)}\right)$, where the values of $\mathcal{E}$ are only computed on $D(\Psi) \subseteq A$ by the recurrence relation (8).

The validity of this algorithm is proved by the following argument. It follows from Main Lemma that $\mathcal{C}\left(\left(h_{\underline{d}}\right)_D\right) = \left(c_{\underline{\psi}}\right)_{\Psi} \iff \left(h_{\underline{d}}\right)_D = \mathcal{C}^{-1}\left(\left(c_{\underline{\psi}}\right)_{\Psi}\right) = \left(\sum_{\underline{\psi} \in \Psi} c_{\underline{\psi}} \underline{\psi}^{\underline{d}}\right)_D$. As $\left(u_{\underline{\psi}}\right)_{\Psi} = \left(c_{\underline{\psi}}\right)_{\Psi} + \left(e_{\underline{\psi}}\right)_{\Psi}$, we have $\left(\widetilde{u}_{\underline{d}}\right)_D = \left(h_{\underline{d}}\right)_D + \left(\sum_{\underline{\psi} \in \Psi} e_{\underline{\psi}} \underline{\psi}^{\underline{d}}\right)_D$ in Step 3 and $\left(\widetilde{u}_{\underline{r}}\right)_R = \left(\sum_{\underline{\psi} \in \Psi} e_{\underline{\psi}} \underline{\psi}^{\underline{r}}\right)_R$ by (14). It follows from the proof of Proposition 2 that $\mathcal{E}\left(\left(\widetilde{u}_{\underline{r}}\right)_R\right) = \left(\sum_{\underline{\psi} \in \Psi} e_{\underline{\psi}} \underline{\psi}^{\underline{d}}\right)_D$ in Step 5, because of which $U = V_R$ is assumed. Thus, we obtain $\left(h_{\underline{d}}\right)_D = \left(\widetilde{u}_{\underline{d}}\right)_D - \left(k_{\underline{d}}\right)_D$ in Step 6.

*Example 8:* (Continued from Example 6) As it can be shown that $d_{\mathrm{FR}} = 7$ for $C^{\perp}(V_R, \Psi)$, the erasure-and-error correction can be performed by Algorithm 1 if $|\Phi_1| + 2|\Phi_2| < 7$. Erasure-and-error decoding of the non-systematic codeword in Fig. 2 via Algorithm 1 is described as follows. The input of Algorithm 1 consists of the received word $\left(u_{\underline{\psi}}\right)_{\Psi}$ in Fig. 4 and a set $\Phi_1$ of erasure locations $\{(\alpha^6, \alpha^4), (\alpha^6, \alpha^7)\}$. Fig. 4 shows the values of vectors at each step in Algorithm 1. In Step 2, the Gröbner basis $\mathcal{G}_{\Phi_1}$ of $Z_{\Phi_1}$ is obtained as

$$\mathcal{G}_{\Phi_1} = \left\{ g^{(0)} = \alpha^2 + x,\ g^{(1)} = \alpha^2 y + xy,\ g^{(2)} = \alpha^3 + \alpha^5 y + y^2 \right\}.$$


$\left(u_{\underline{\psi}}\right)_{\Psi}$
Step 1
$\left(v_{\underline{r}}\right)_{R}$
Step 3
$\left(\tilde{u}_{\underline{d}}\right)_{D}$
Step 5
$\left(k_{\underline{d}}\right)_{D}$
Step 6
$\left(h_{\underline{d}}\right)_{D}$

$\left(u_{\underline{\psi}}\right)_{\Psi}$

| | -1 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|---|
| -1 | 3 | | | 4 | | | | 1 | |
| 0 | | | | | | 7 | 0 | | 7 |
| 1 | | 1 | 4 | | 5 | | | | |
| 2 | | | | | | 4 | 0 | | 4 |
| 3 | | 6 | -1 | | 1 | | | | |
| 4 | | | | | | 3 | 7 | | 7 |
| 5 | | 0 | 7 | | 7 | | | | |
| 6 | | | | | | 5 | 6 | | 5 |
| 7 | | 2 | 5 | | 6 | | | | |

$\left(v_{\underline{r}}\right)_{R}$

| | 0 | 1 | 2 |
|---|---|---|---|
| 0 | 4 | 1 | 1 |
| 1 | 2 | 7 | 7 |
| 2 | 0 | 5 | |
| 3 | 6 | | |

$\left(\tilde{u}_{\underline{d}}\right)_{D}$

| | 0 | 1 | 2 |
|---|---|---|---|
| 0 | 2 | 5 | 5 |
| 1 | 5 | 5 | 2 |
| 2 | 4 | 4 | 3 |
| 3 | 5 | 4 | 1 |
| 4 | 2 | 6 | 4 |
| 5 | 6 | 1 | 2 |
| 6 | 2 | 4 | 2 |
| 7 | 5 | -1 | 7 |
| 8 | 5 | -1 | 4 |

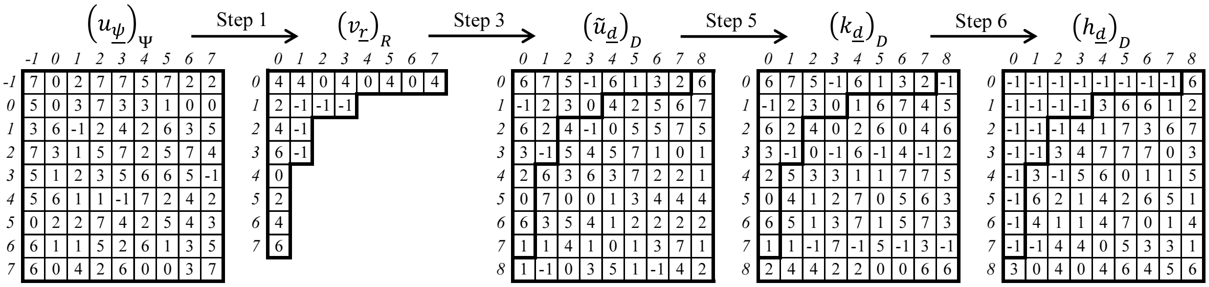
$\left(k_{\underline{d}}\right)_{D}$

| | 0 | 1 | 2 |
|---|---|---|---|
| 0 | 2 | 5 | 5 |
| 1 | 5 | 5 | 2 |
| 2 | 4 | 4 | 7 |
| 3 | 5 | 5 | 3 |
| 4 | -1 | -1 | 2 |
| 5 | 2 | 2 | 3 |
| 6 | 2 | 2 | -1 |
| 7 | 4 | 4 | 0 |
| 8 | 1 | 1 | 0 |

$\left(h_{\underline{d}}\right)_{D}$

| | 0 | 1 | 2 |
|---|---|---|---|
| 0 | -1 | -1 | -1 |
| 1 | -1 | -1 | -1 |
| 2 | -1 | -1 | 7 |
| 3 | -1 | 6 | 2 |
| 4 | 2 | 6 | 7 |
| 5 | 2 | 3 | 4 |
| 6 | -1 | 7 | 2 |
| 7 | 2 | 0 | 1 |
| 8 | 1 | 5 | 0 |

Fig. 4. Numerical example of Algorithm 1 for a non-systematic Hermitian codeword with erasure-and-errors. The Gröbner bases are shown in Example 8.


$\left(u_{\underline{\psi}}\right)_{\Psi}$
Step 1
$\left(v_{\underline{r}}\right)_{R}$
Step 3
$\left(\tilde{u}_{\underline{d}}\right)_{D}$
Step 5
$\left(k_{\underline{d}}\right)_{D}$
Step 6
$\left(h_{\underline{d}}\right)_{D}$

$\left(u_{\underline{\psi}}\right)_{\Psi}$

| | -1 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|---|
| -1 | 7 | 0 | 2 | 7 | 7 | 5 | 7 | 2 | 2 |
| 0 | 5 | 0 | 3 | 7 | 3 | 3 | 1 | 0 | 0 |
| 1 | 3 | 6 | -1 | 2 | 4 | 2 | 6 | 3 | 5 |
| 2 | 7 | 3 | 1 | 5 | 7 | 2 | 5 | 7 | 4 |
| 3 | 5 | 1 | 2 | 3 | 5 | 6 | 6 | 5 | -1 |
| 4 | 5 | 6 | 1 | 1 | -1 | 7 | 2 | 4 | 2 |
| 5 | 0 | 2 | 2 | 7 | 4 | 2 | 5 | 4 | 3 |
| 6 | 6 | 1 | 1 | 5 | 2 | 6 | 1 | 3 | 5 |
| 7 | 6 | 0 | 4 | 2 | 6 | 0 | 0 | 3 | 7 |

$\left(v_{\underline{r}}\right)_{R}$

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| 0 | 4 | 4 | 0 | 4 | 0 | 4 | 0 | 4 |
| 1 | 2 | -1 | -1 | -1 | | | | |
| 2 | 4 | -1 | | | | | | |
| 3 | 6 | -1 | | | | | | |
| 4 | 0 | | | | | | | |
| 5 | 2 | | | | | | | |
| 6 | 4 | | | | | | | |
| 7 | 6 | | | | | | | |

$\left(\tilde{u}_{\underline{d}}\right)_{D}$

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|---|
| 0 | 6 | 7 | 5 | -1 | 6 | 1 | 3 | 2 | 6 |
| 1 | -1 | 2 | 3 | 0 | 4 | 2 | 5 | 6 | 7 |
| 2 | 6 | 2 | 4 | -1 | 0 | 5 | 5 | 7 | 5 |
| 3 | 3 | -1 | 5 | 4 | 5 | 7 | 1 | 0 | 1 |
| 4 | 2 | 6 | 3 | 6 | 3 | 7 | 2 | 2 | 1 |
| 5 | 0 | 7 | 0 | 0 | 1 | 3 | 4 | 4 | 4 |
| 6 | 6 | 3 | 5 | 4 | 1 | 2 | 2 | 2 | 2 |
| 7 | 1 | 1 | 4 | 1 | 0 | 1 | 3 | 7 | 1 |
| 8 | 1 | -1 | 0 | 3 | 5 | 1 | -1 | 4 | 2 |

$\left(k_{\underline{d}}\right)_{D}$

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|---|
| 0 | 6 | 7 | 5 | -1 | 6 | 1 | 3 | 2 | -1 |
| 1 | -1 | 2 | 3 | 0 | 1 | 6 | 7 | 4 | 5 |
| 2 | 6 | 2 | 4 | 0 | 2 | 6 | 0 | 4 | 6 |
| 3 | 3 | -1 | 0 | -1 | 6 | -1 | 4 | -1 | 2 |
| 4 | 2 | 5 | 3 | 3 | 1 | 1 | 7 | 7 | 5 |
| 5 | 0 | 4 | 1 | 2 | 7 | 0 | 5 | 6 | 3 |
| 6 | 6 | 5 | 1 | 3 | 7 | 1 | 5 | 7 | 3 |
| 7 | 1 | 1 | -1 | 7 | -1 | 5 | -1 | 3 | -1 |
| 8 | 2 | 4 | 4 | 2 | 2 | 0 | 0 | 6 | 6 |

$\left(h_{\underline{d}}\right)_{D}$

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|---|
| 0 | -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 | 6 |
| 1 | -1 | -1 | -1 | -1 | 3 | 6 | 6 | 1 | 2 |
| 2 | -1 | -1 | -1 | 4 | 1 | 7 | 3 | 6 | 7 |
| 3 | -1 | -1 | 3 | 4 | 7 | 7 | 7 | 0 | 3 |
| 4 | -1 | 3 | -1 | 5 | 6 | 0 | 1 | 1 | 5 |
| 5 | -1 | 6 | 2 | 1 | 4 | 2 | 6 | 5 | 1 |
| 6 | -1 | 4 | 1 | 1 | 4 | 7 | 0 | 1 | 4 |
| 7 | -1 | -1 | 4 | 4 | 0 | 5 | 3 | 3 | 1 |
| 8 | 3 | 0 | 4 | 0 | 4 | 6 | 4 | 5 | 6 |

Fig. 5. Numerical example of Algorithm 1 for a non-systematic HCRS codeword with erasure-and-errors. The Gröbner bases are shown in Example 9.

In Step 4, the Gröbner basis $\mathcal{G}_{\Phi_1 \cup \Phi_2}$ of $Z_{\Phi_1 \cup \Phi_2}$ is obtained as

$$\mathcal{G}_{\Phi_1 \cup \Phi_2} = \left\{ \begin{array}{l} g^{(0)} = \alpha x + \alpha^4 x^2 + x^3, \\ g^{(1)} = 1 + \alpha^7 x + \alpha^2 y + \alpha^2 x^2 + xy, \\ g^{(2)} = \alpha^5 + \alpha^7 x + \alpha^5 y + \alpha^2 x^2 + y^2 \end{array} \right\}.$$

If we perform Chien search for $\mathcal{G}_{\Phi_1 \cup \Phi_2}$, the set $\Phi_1 \cup \Phi_2$ of the erasure-and-error locations can be determined; however, the explicit set $\Phi_1 \cup \Phi_2$ may not be used in our algorithm. It can be seen in Fig. 4 that the erasure-and-error spectrum $\left(k_{\underline{d}}\right)_D$ is generated by $\mathcal{G}_{\Phi_1 \cup \Phi_2}$ from $\left(\widetilde{u}_{\underline{r}}\right)_R$ in Step 5, and is then removed from $\left(\widetilde{u}_{\underline{d}}\right)_D$ in Step 6. The resulting $\left(h_{\underline{d}}\right)_D$ agrees with the information given in Fig. 2. □

*Example 9:* (Continued from Example 7) As it can be shown [13] that $d_{\min} = d_{\mathrm{FR}} = 9$ for $C^{\perp}(V_R, \Psi)$, where $d_{\min}$ is the true minimum distance, the erasure-and-error correction can be performed by Algorithm 1 if $|\Phi_1| + 2|\Phi_2| < 9$. Fig. 5 shows the data at each step of Algorithm 1 for the erasure-and-error decoding of the non-systematic codeword in Fig. 3. The input of Algorithm 1 consists of the received word $\left(u_{\underline{\psi}}\right)_{\Psi}$ in Fig. 5 and a set $\Phi_1$ of erasure locations $\{(0, \alpha^4), (\alpha^2, 0)\}$. Consider the graded lexicographic order [6] to be a monomial order $\preceq$ such that $(a, b) \preceq (a', b') \Leftrightarrow a + b < a' + b'$ or $a + b = a' + b'$, $a \leq a'$, i.e., $(0,0) \preceq (1,0) \preceq (0,1) \preceq (2,0) \preceq (1,1) \preceq (0,2) \preceq (3,0) \preceq \cdots \preceq (0,3) \preceq (4,0) \preceq (3,1) \preceq \cdots \preceq (8,8)$ on $A = [0,8]^2$. In Step 2, the Gröbner basis

$\mathcal{G}_{\Phi_1}$ of $Z_{\Phi_1}$ is obtained as

$$\mathcal{G}_{\Phi_1} = \left\{ g^{(0)} = \alpha^6 x + x^2,\ g^{(1)} = \alpha^0 + \alpha^2 x + y \right\}.$$

In Step 4, the Gröbner basis $\mathcal{G}_{\Phi_1 \cup \Phi_2}$ of $Z_{\Phi_1 \cup \Phi_2}$ is obtained as

$$\mathcal{G}_{\Phi_1 \cup \Phi_2} = \left\{ \begin{array}{l} g^{(0)} = \alpha^6 + \alpha^6 y + \alpha^2 x^2 + xy + x^3, \\ g^{(1)} = 1 + \alpha x + y + \alpha^5 x^2 + x^2 y, \\ g^{(2)} = 1 + \alpha x + \alpha^4 y + \alpha^5 x^2 + \alpha^3 xy + y^2 \end{array} \right\}.$$

The resulting $\left(h_{\underline{d}}\right)_D$ agrees with the information given in Fig. 3. □

### C. *Erasure-and-error decoding: general case*

In Algorithm 1, we removed the erasure-and-error spectrum from the received word spectrum without identifying $\left(e_{\underline{\psi}}\right)_\Psi$. In this subsection, we consider the problem of erasure-and-error decoding with identifying $\left(e_{\underline{\psi}}\right)_\Psi$ in the received word. It follows from Main Lemma that the value of $\mathcal{C}$ for the erasure-and-error spectrum is equal to $\left(e_{\underline{\psi}}\right)_\Psi$. Though $\mathcal{F}^{-1}$ was not used in Algorithm 1, the map $\mathcal{C}$ including $\mathcal{F}^{-1}$ is required in Algorithm 2.

```
Algorithm 2: (Finding erasures and errors)
Input: $\Phi_1$ and a received word $\left(u_{\underline{\psi}}\right)_\Psi \in V_\Psi$
Output: $\left(c_{\underline{\psi}}\right)_\Psi \in C^\perp(V_R, \Psi)$
Step 1. $\left(v_{\underline{r}}\right)_R = \left(\sum_{\underline{\phi} \in \Phi_1} \underline{\phi}^{\underline{r}}\right)_R$
Step 2. Calculate $\mathcal{G}_{\Phi_1}$ from syndrome $\left(v_{\underline{r}}\right)_R$
Step 3. $\left(\widetilde{u}_{\underline{r}}\right)_R = \left(\sum_{\underline{\psi} \in \Psi} u_{\underline{\psi}} \underline{\psi}^{\underline{r}}\right)_R$
Step 4. Calculate $\mathcal{G}_{\Phi_1 \cup \Phi_2}$ from $\left(\widetilde{u}_{\underline{r}}\right)_R$ and $\mathcal{G}_{\Phi_1}$
Step 5. $\left(e_{\underline{\psi}}\right)_\Psi = \mathcal{C}\left(\left(\widetilde{u}_{\underline{r}}\right)_R\right)$
Step 6. $\left(c_{\underline{\psi}}\right)_\Psi = \left(u_{\underline{\psi}}\right)_\Psi - \left(e_{\underline{\psi}}\right)_\Psi$ □
```

In this algorithm, Main Lemma is used in Step 5, because $\left(\widetilde{u}_{\underline{r}}\right)_R = \left(\sum_{\underline{\psi} \in \Psi} e_{\underline{\psi}} \underline{\psi}^{\underline{r}}\right)_R = \mathcal{C}^{-1}\left(\left(e_{\underline{\psi}}\right)_\Psi\right)$ from definition (14), and $\mathcal{C}\left(\left(\widetilde{u}_{\underline{r}}\right)_R\right) = \left(e_{\underline{\psi}}\right)_\Psi$ by Main Lemma, which is applied as $\mathcal{C} : V_D \to V_{\Phi_1 \cup \Phi_2}$ with $D = D(\Phi_1 \cup \Phi_2)$. Note that $\left(e_{\underline{\psi}}\right)_{\Phi_1 \cup \Phi_2} = \mathcal{C}\left(\left(\widetilde{u}_{\underline{d}}\right)_D\right)$ is denoted as $\left(e_{\underline{\psi}}\right)_\Psi = \mathcal{C}\left(\left(\widetilde{u}_{\underline{r}}\right)_R\right)$ because $V_{\Phi_1 \cup \Phi_2} \subseteq V_\Psi$ and $D(\Phi_1 \cup \Phi_2) \subseteq R$.

*Example 10:* (Continued from Example 8) Erasure-and-error decoding of the codeword in Fig. 2 via Algorithm 2 is described as follows. The input of Algorithm 2 is the same as for Example 8. Fig. 6 shows the values of vectors at each step of Algorithm 2. The Gröbner basis $\mathcal{G}_{\Phi_1}$ in Step 2 and the Gröbner basis $\mathcal{G}_{\Phi_1 \cup \Phi_2}$ in Step 4 are the same as those in Example 8. Although $\mathcal{C}$ is used in Step 5 of Algorithm 2, the value of $\mathcal{E}\left(\left(\widetilde{u}_{\underline{d}}\right)_D\right)$ is given in Fig. 6 in order to show the process. □

*Example 11:* (Continued from Example 9) Erasure-and-error decoding of the codeword in Fig. 3 via Algorithm 2 is described as follows. The input of Algorithm 2 is the same as for Example 9. All data at each step of Algorithm

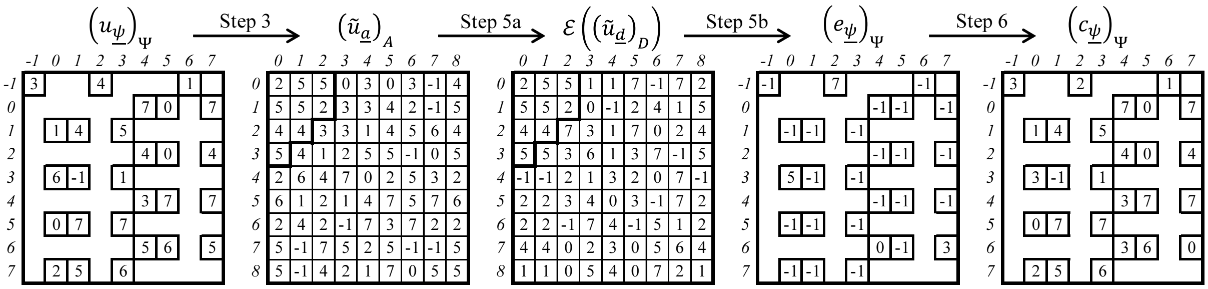

$\left(u_{\underline{\psi}}\right)_\Psi$
Step 3
$\left(\tilde{u}_{\underline{a}}\right)_A$
Step 5a
$\mathcal{E}\left(\left(\tilde{u}_{\underline{d}}\right)_D\right)$
Step 5b
$\left(e_{\underline{\psi}}\right)_\Psi$
Step 6
$\left(c_{\underline{\psi}}\right)_\Psi$

Fig. 6. Numerical example of Algorithm 2 for a Hermitian codeword with erasure-and-error, cf. Example 10. Although only $\left(\tilde{u}_{\underline{r}}\right)_R$ is required, $\left(\tilde{u}_{\underline{a}}\right)_A$ is shown for consistency and for the discussion in Subsection VI-B. The delta set $D$ in $\mathcal{E}\left(\left(\tilde{u}_{\underline{d}}\right)_D\right)$ indicates $D(\Phi_1 \cup \Phi_2)$ and $\mathcal{E}$ is formed from $\mathcal{G}_{\Phi_1 \cup \Phi_2}$.

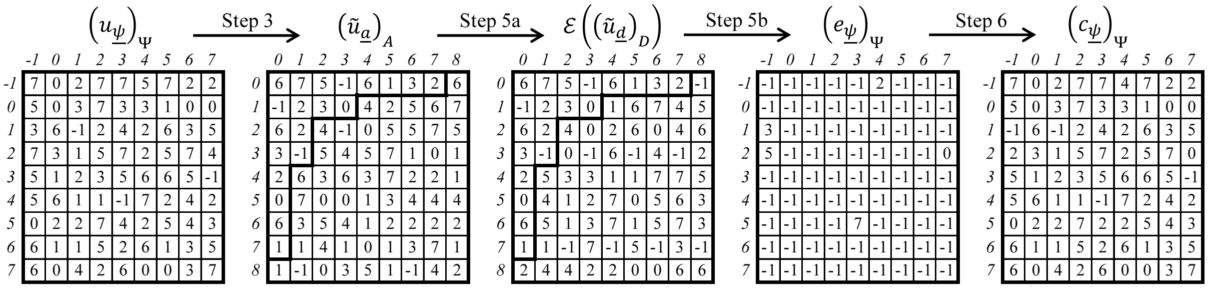

$\left(u_{\underline{\psi}}\right)_\Psi$
Step 3
$\left(\tilde{u}_{\underline{a}}\right)_A$
Step 5a
$\mathcal{E}\left(\left(\tilde{u}_{\underline{d}}\right)_D\right)$
Step 5b
$\left(e_{\underline{\psi}}\right)_\Psi$
Step 6
$\left(c_{\underline{\psi}}\right)_\Psi$

Fig. 7. Numerical example of Algorithm 2 for an HCRS codeword with erasure-and-error, cf. Example 11. As noted in Example 10, $\mathcal{E}\left(\left(\tilde{u}_{\underline{d}}\right)_D\right)$ is the computational process of $\mathcal{C} = \mathcal{F}^{-1} \circ \mathcal{E}$ in Step 5 of Algorithm 2. A received word $\left(u_{\underline{\psi}}\right)_\Psi$ is decomposed into $\left(e_{\underline{\psi}}\right)_\Psi$ and $\left(c_{\underline{\psi}}\right)_\Psi$.

2 are shown in Fig. 7. The Gröbner basis $\mathcal{G}_{\Phi_1}$ in Step 2 and the Gröbner basis $\mathcal{G}_{\Phi_1 \cup \Phi_2}$ in Step 4 are the same as those in Example 9. □

*Remark 4:* One might consider that, as the Gröbner basis $\mathcal{G}_{\Phi_1 \cup \Phi_2}$ is obtained in Step 4 of Algorithms 1 and 2, and the set $\Phi_1 \cup \Phi_2$ of erasure-and-error locations can be calculated by Chien search, the erasure-and-error values $\left(e_{\underline{\psi}}\right)_{\Phi_1 \cup \Phi_2}$ can be computed from the system of linear equations $\left(\sum_{\underline{\phi} \in \Phi_1 \cup \Phi_2} e_{\underline{\phi}} \underline{\phi}^{\underline{d}}\right)_D = \left(\tilde{u}_{\underline{d}}\right)_D$ with $D = D(\Phi_1 \cap \Phi_2)$, the matrix of which is invertible by (4) and Appendix C. If we use Gaussian elimination to solve this, then the computational complexity is of the order $(t+u)^3$, which is bounded by $n^3$. We will see in the next section that the computational complexity of Step 5 in Algorithm 1 or 2 for finding the erasure-and-error values or spectrum is bounded by the order $qn^{2+\varepsilon}$ with any $0 < \varepsilon < 1$. Consequently, we can choose an appropriate method according to $t + u$ and $n$. □

### D. Systematic encoding regarded as erasure-only decoding

Because, in practical use, error-correcting codes are usually encoded systematically, it is natural to consider the systematic encoding of $C^\perp(V_R, \Psi)$. In this subsection, we show that the systematic encoding is equivalent to a certain type of erasure-only decoding under Algorithm 2.

Systematic encoding means that there exists at least one $\Phi$ with $\Phi \subseteq \Psi$ and $|\Phi| = |R|$ such that, for any given information $\left(h_{\underline{\psi}}\right)_{\Psi\backslash\Phi}$, we find $\left(c_{\underline{\psi}}\right)_{\Psi} \in C^{\perp}(V_R,\Psi)$ with $c_{\underline{\psi}} = h_{\underline{\psi}}$ for all $\underline{\psi} \in \Psi\backslash\Phi$. Thus, $\Phi$ corresponds to the set of redundant locations, and $\Psi\backslash\Phi$ corresponds to the set of information locations, in the codewords of $C^{\perp}(V_R,\Psi)$. If $\Phi$ is fixed, then systematic encoding can be viewed as the erasure-only decoding of $\left(e_{\underline{\phi}}\right)_{\Phi} = \left(-c_{\underline{\phi}}\right)_{\Phi}$. However, as $|\Phi_1| = n-k = |\Phi|$ and $|\Phi_2| = 0$, the correctable erasure-and-error bound $|\Phi_1| + 2|\Phi_2| < d_{\mathrm{FR}}$ is not generally valid.

*Example 12:* (Continued from Examples 8 and 9) In Examples 6 and 8, because $|R| = n-k = 9$ and $d_{\mathrm{FR}} = 7$ for the Hermitian code, the correctable erasure-only bound $|R| = |\Phi_1| < d_{\mathrm{FR}}$ is not valid. Similarly, in Examples 7 and 9, because $|R| = n-k = 20$ and $d_{\mathrm{FR}} = 9$ for the extended HCRS code, the correctable erasure-only bound $|R| = |\Phi_1| < d_{\mathrm{FR}}$ is also not valid. □

Nevertheless, we can show that, in many cases, there exists $\Phi$ such that the systematic encoding works as an erasure-only decoding on $\Phi$. We now state the condition for the erasure-only decoding under Algorithm 2 with $|\Phi| = |R|$.

*Corollary : (Erasure-only decodable condition)* Suppose that an erasure-only $\left(e_{\underline{\psi}}\right)_{\Psi}$ has occurred in a received word $\left(u_{\underline{\psi}}\right)_{\Psi} = \left(c_{\underline{\psi}}\right)_{\Psi} + \left(e_{\underline{\psi}}\right)_{\Psi}$ from some channel, where $\left(e_{\underline{\psi}}\right)_{\Psi}$ is unknown, but $\Phi \subseteq \Psi$ is known and $e_{\underline{\psi}} \neq 0 \Rightarrow \underline{\psi} \in \Phi$. If the linear map $\mathrm{ev}\,|_{V_R,\Phi}$ given by

$$\mathrm{ev}\,|_{V_R,\Phi}\colon V_R \to V_\Phi \qquad \left[\left(h_{\underline{r}}\right)_R \mapsto \left(\sum_{\underline{r}\in R} h_{\underline{r}}\underline{\phi}^{\underline{r}}\right)_{\Phi}\right] \tag{17}$$

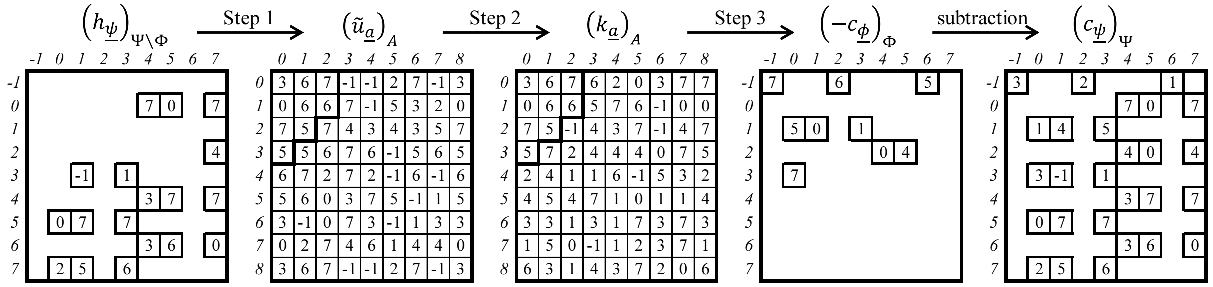
is isomorphic, then the received word $\left(u_{\underline{\psi}}\right)_{\Psi}$ can be decoded by Algorithm 2. □
Note that this condition is equivalent to $\det\left[\underline{x}_l\left(\underline{\phi}_m\right)\right] \neq 0$, where $\{\underline{x}^{\underline{r}} \,|\, \underline{r} \in R\} = \{\underline{x}_l \mid 1 \le l \le |R|\}$ and $\Phi = \left\{\underline{\phi}_m \,\middle|\, 1 \le m \le |\Phi|\right\}$ are aligned in any order, and $\underline{x}_l\left(\underline{\phi}_m\right)$ is the $(l,m)$-th entry. This matrix is considered in Appendix C. A non-zero determinant value is expected to occur with high probability $(q-1)/q$.

The validity of this Corollary can be described directly as follows. Let $\Phi \subseteq \Psi \subseteq \Omega$, so that (17) is isomorphic. It follows from the surjectivity of (17) that, for any $\underline{a} \in A\backslash R$, there exists $\left(h_{\underline{r}}\right)_R \in V_R$ such that $\left(\sum_{\underline{r}\in R} h_{\underline{r}}\underline{\phi}^{\underline{r}}\right)_{\Phi} = \left(-\underline{\phi}^{\underline{a}}\right)_{\Phi}$. We can then find $f \in \mathbb{F}_q[\underline{x}]$ such that $f\left(\underline{\phi}\right) = 0$ for all $\underline{\phi} \in \Phi$; actually, $f$ is given by

$$f = f(\underline{x}) = \underline{x}^{\underline{a}} + \sum_{\underline{r}\in R} h_{\underline{r}}\underline{x}^{\underline{r}} \in \mathbb{F}_q[\underline{x}].$$

Because $\underline{a} \in A\backslash R$ is arbitrary, the $\mathcal{G}_\Phi = \left\{f^{(w)}\right\}_{0\le w<b}$ obtained is sufficient to extend $V_R$ into $V_A$ via $\mathcal{E}$ by (7) and (8); $b$ can be taken as, at most, $b \le q^{N-1}$ if $|A| = q^N$. The syndrome $\left(\sum_{\underline{\psi}\in\Psi} u_{\underline{\psi}}\underline{\psi}^{\underline{r}}\right)_R = \left(\sum_{\underline{\phi}\in\Phi} e_{\underline{\phi}}\underline{\phi}^{\underline{r}}\right)_R$ can then be extended into $\mathcal{E}\left(\left(\sum_{\underline{\phi}\in\Phi} e_{\underline{\phi}}\underline{\phi}^{\underline{r}}\right)_R\right) = \left(\sum_{\underline{\phi}\in\Phi} e_{\underline{\phi}}\underline{\phi}^{\underline{a}}\right)_A$ by Proposition 2, and by function $\mathcal{R}\circ\mathcal{F}^{-1}$, we obtain $\mathcal{C}\left(\left(\sum_{\underline{\phi}\in\Phi} e_{\underline{\phi}}\underline{\phi}^{\underline{r}}\right)_R\right) = \left(e_{\underline{\phi}}\right)_{\Phi}$ by Main Lemma.

The computation of $\mathcal{G}_\Phi$ can be performed by the BMS algorithm; for systematic encoding, we calculate the $\mathcal{G}_\Phi$ in advance—these play the role of generator polynomials in the case of Reed–Solomon codes. Although the following Algorithm 3 is equivalent to a special case of Algorithm 2 for $\Phi_1 = \Phi$ and $\Phi_2 = \emptyset$, we give it separately to describe systematic encoding.



$\left(h_{\underline{\psi}}\right)_{\Psi\setminus\Phi}$

| | -1 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|---|
| -1 | | | | | | | | | |
| 0 | | | | | | 7 | 0 | | 7 |
| 1 | | | | | | | | | |
| 2 | | | | | | | | | 4 |
| 3 | | | -1 | | 1 | | | | |
| 4 | | | | | | 3 | 7 | | 7 |
| 5 | | 0 | 7 | | 7 | | | | |
| 6 | | | | | | 3 | 6 | | 0 |
| 7 | | 2 | 5 | | 6 | | | | |

$\left(\tilde{u}_{\underline{a}}\right)_A$

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|---|
| 0 | 3 | 6 | 7 | -1 | -1 | 2 | 7 | -1 | 3 |
| 1 | 0 | 6 | 6 | 7 | -1 | 5 | 3 | 2 | 0 |
| 2 | 7 | 5 | 7 | 4 | 3 | 4 | 3 | 5 | 7 |
| 3 | 5 | 5 | 6 | 7 | 6 | -1 | 5 | 6 | 5 |
| 4 | 6 | 7 | 2 | 7 | 2 | -1 | 6 | -1 | 6 |
| 5 | 5 | 6 | 0 | 3 | 7 | 5 | -1 | 1 | 5 |
| 6 | 3 | -1 | 0 | 7 | 3 | -1 | 1 | 3 | 3 |
| 7 | 0 | 2 | 7 | 4 | 6 | 1 | 4 | 4 | 0 |
| 8 | 3 | 6 | 7 | -1 | -1 | 2 | 7 | -1 | 3 |

$\left(k_{\underline{a}}\right)_A$

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|---|
| 0 | 3 | 6 | 7 | 6 | 2 | 0 | 3 | 7 | 7 |
| 1 | 0 | 6 | 6 | 5 | 7 | 6 | -1 | 0 | 0 |
| 2 | 7 | 5 | -1 | 4 | 3 | 7 | -1 | 4 | 7 |
| 3 | 5 | 7 | 2 | 4 | 4 | 4 | 0 | 7 | 5 |
| 4 | 2 | 4 | 1 | 1 | 6 | -1 | 5 | 3 | 2 |
| 5 | 4 | 5 | 4 | 7 | 1 | 0 | 1 | 1 | 4 |
| 6 | 3 | 3 | 1 | 3 | 1 | 7 | 3 | 7 | 3 |
| 7 | 1 | 5 | 0 | -1 | 1 | 2 | 3 | 7 | 1 |
| 8 | 6 | 3 | 1 | 4 | 3 | 7 | 2 | 0 | 6 |

$\left(-c_{\underline{\phi}}\right)_{\Phi}$

| | -1 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|---|
| -1 | 7 | | | 6 | | | | 5 | |
| 0 | | | | | | | | | |
| 1 | | 5 | 0 | | 1 | | | | |
| 2 | | | | | | 0 | 4 | | |
| 3 | | 7 | | | | | | | |
| 4 | | | | | | | | | |
| 5 | | | | | | | | | |
| 6 | | | | | | | | | |
| 7 | | | | | | | | | |

$\left(c_{\underline{\psi}}\right)_{\Psi}$

| | -1 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|---|
| -1 | 3 | | | 2 | | | | 1 | |
| 0 | | | | | | 7 | 0 | | 7 |
| 1 | | 1 | 4 | | 5 | | | | |
| 2 | | | | | | 4 | 0 | | 4 |
| 3 | | 3 | -1 | | 1 | | | | |
| 4 | | | | | | 3 | 7 | | 7 |
| 5 | | 0 | 7 | | 7 | | | | |
| 6 | | | | | | 3 | 6 | | 0 |
| 7 | | 2 | 5 | | 6 | | | | |

Fig. 8. Numerical example of systematic encoding of the Hermitian code $C^{\perp}(V_R, \Psi)$ by Algorithm 3, where $\Phi$ is given by (18) and the Gröbner basis $\mathcal{G}_{\Phi}$ is described in Example 13. The given information $\left(h_{\underline{\psi}}\right)_{\Psi\setminus\Phi}$ is systematically encoded into a codeword $\left(c_{\underline{\psi}}\right)_{\Psi}$.

```
*Algorithm 3: (DFT systematic encoding)*
Input: $\Phi$ and an information word $\left(h_{\underline{\psi}}\right)_{\Psi\setminus\Phi}$
Output: $\left(c_{\underline{\psi}}\right)_{\Psi} \in C^{\perp}(V_R, \Psi)$ with $\left(c_{\underline{\psi}}\right)_{\Psi\setminus\Phi} = \left(h_{\underline{\psi}}\right)_{\Psi\setminus\Phi}$
Step 1. $\left(\widetilde{u}_{\underline{r}}\right)_R = \left(\sum_{\underline{\psi}\in\Psi\setminus\Phi} h_{\underline{\psi}}\underline{\psi}^{\underline{r}}\right)_R$
Step 2. $\left(k_{\underline{a}}\right)_A = \mathcal{E}\left(\left(\widetilde{u}_{\underline{r}}\right)_R\right)$ by $\mathcal{G}_{\Phi}$
Step 3. $\left(c_{\underline{\phi}}\right)_{\Phi} = -\mathcal{R}\circ\mathcal{F}^{-1}\left(\left(k_{\underline{a}}\right)_A\right)$  □
```

*Example 13:* (Continued from Example 12) Let

$$\Phi = \left\{ \begin{array}{c} (0,0),(0,\alpha^2),(0,\alpha^6),(\alpha,1),(\alpha,\alpha), \\ (\alpha,\alpha^3),(\alpha^2,\alpha^4),(\alpha^2,\alpha^5),(\alpha^3,1) \end{array} \right\}. \tag{18}$$

The Gröbner basis $\mathcal{G}_{\Phi} = \left\{g^{(0)}, g^{(1)}, g^{(2)}, g^{(3)}\right\}$ is given by

$$g^{(0)} = \alpha^2 x + \alpha^7 x^2 + \alpha x^3 + x^4,$$

$$g^{(1)} = \alpha^7 x + x^2 + \alpha^4 x^3 + y(\alpha^3 x + \alpha^4 x^2 + x^3),$$

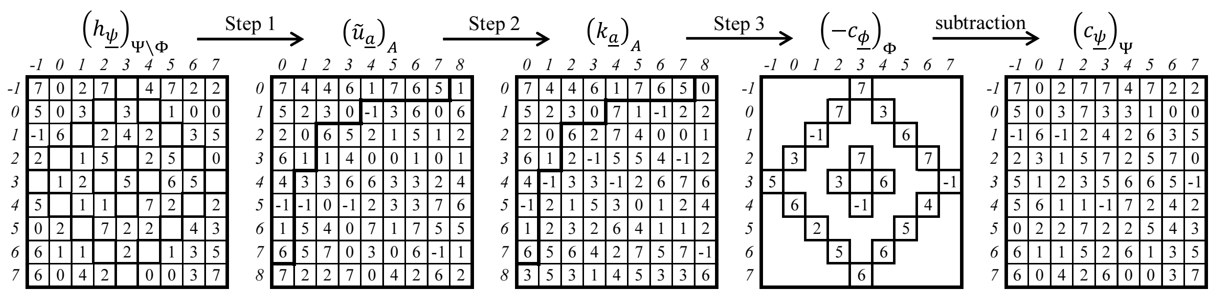
$$g^{(2)} = \alpha^4 x^2 + \alpha^7 x^3 + y(\alpha^4 x + \alpha^7 x^2) + y^2(\alpha^5 x + x^2),$$

$$g^{(3)} = \alpha^2 x + \alpha^7 x^2 + \alpha x^3 + y + y^3.$$

As $D(\Phi) = R$, the isomorphy of (17) follows from (4). All values of Algorithm 3 are shown in Fig. 8. □

*Example 14:* (Continued from Example 12) Let

$$\Phi = \left\{ \begin{array}{c} (0,\alpha^3),(1,\alpha^2),(1,\alpha^4),(\alpha,\alpha),(\alpha,\alpha^5), \\ (\alpha^2,1),(\alpha^2,\alpha^3),(\alpha^2,\alpha^6),(\alpha^3,0),(\alpha^3,\alpha^2), \\ (\alpha^3,\alpha^4),(\alpha^3,\alpha^7),(\alpha^4,1),(\alpha^4,\alpha^3),(\alpha^4,\alpha^6), \\ (\alpha^5,\alpha),(\alpha^5,\alpha^5),(\alpha^6,\alpha^2),(\alpha^6,\alpha^4),(\alpha^7,\alpha^3) \end{array} \right\}; \tag{19}$$


$\left(h_{\underline{\psi}}\right)_{\Psi\setminus\Phi}$
Step 1
$\left(\tilde{u}_{\underline{a}}\right)_A$
Step 2
$\left(k_{\underline{a}}\right)_A$
Step 3
$\left(-c_{\underline{\phi}}\right)_\Phi$
subtraction
$\left(c_{\underline{\psi}}\right)_\Psi$

$\left(h_{\underline{\psi}}\right)_{\Psi\setminus\Phi}$

|  | -1 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|---|
| -1 | 7 | 0 | 2 | 7 |  | 4 | 7 | 2 | 2 |
| 0 | 5 | 0 | 3 |  | 3 |  | 1 | 0 | 0 |
| 1 | -1 | 6 |  | 2 | 4 | 2 |  | 3 | 5 |
| 2 | 2 |  | 1 | 5 |  | 2 | 5 |  | 0 |
| 3 |  | 1 | 2 |  | 5 |  | 6 | 5 |  |
| 4 | 5 |  | 1 | 1 |  | 7 | 2 |  | 2 |
| 5 | 0 | 2 |  | 7 | 2 | 2 |  | 4 | 3 |
| 6 | 6 | 1 | 1 |  | 2 |  | 1 | 3 | 5 |
| 7 | 6 | 0 | 4 | 2 |  | 0 | 0 | 3 | 7 |

$\left(\tilde{u}_{\underline{a}}\right)_A$

|  | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|---|
| 0 | 7 | 4 | 4 | 6 | 1 | 7 | 6 | 5 | 1 |
| 1 | 5 | 2 | 3 | 0 | -1 | 3 | 6 | 0 | 6 |
| 2 | 2 | 0 | 6 | 5 | 2 | 1 | 5 | 1 | 2 |
| 3 | 6 | 1 | 1 | 4 | 0 | 0 | 1 | 0 | 1 |
| 4 | 4 | 3 | 3 | 6 | 6 | 3 | 3 | 2 | 4 |
| 5 | -1 | -1 | 0 | -1 | 2 | 3 | 3 | 7 | 6 |
| 6 | 1 | 5 | 4 | 0 | 7 | 1 | 7 | 5 | 5 |
| 7 | 6 | 5 | 7 | 0 | 3 | 0 | 6 | -1 | 1 |
| 8 | 7 | 2 | 2 | 7 | 0 | 4 | 2 | 6 | 2 |

$\left(k_{\underline{a}}\right)_A$

|  | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|---|
| 0 | 7 | 4 | 4 | 6 | 1 | 7 | 6 | 5 | 0 |
| 1 | 5 | 2 | 3 | 0 | 7 | 1 | -1 | 2 | 2 |
| 2 | 2 | 0 | 6 | 2 | 7 | 4 | 0 | 0 | 1 |
| 3 | 6 | 1 | 2 | -1 | 5 | 5 | 4 | -1 | 2 |
| 4 | 4 | -1 | 3 | 3 | -1 | 2 | 6 | 7 | 6 |
| 5 | -1 | 2 | 1 | 5 | 3 | 0 | 1 | 2 | 4 |
| 6 | 1 | 2 | 3 | 2 | 6 | 4 | 1 | 1 | 2 |
| 7 | 6 | 5 | 6 | 4 | 2 | 7 | 5 | 7 | -1 |
| 8 | 3 | 5 | 3 | 1 | 4 | 5 | 3 | 3 | 6 |

$\left(-c_{\underline{\phi}}\right)_\Phi$

|  | -1 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|---|
| -1 |  |  |  |  | 7 |  |  |  |  |
| 0 |  |  |  | 7 |  | 3 |  |  |  |
| 1 |  |  | -1 |  |  |  | 6 |  |  |
| 2 |  | 3 |  |  | 7 |  |  | 7 |  |
| 3 | 5 |  |  | 3 |  | 6 |  |  | -1 |
| 4 |  | 6 |  |  | -1 |  |  | 4 |  |
| 5 |  |  | 2 |  |  |  | 5 |  |  |
| 6 |  |  |  | 5 |  | 6 |  |  |  |
| 7 |  |  |  |  | 6 |  |  |  |  |

$\left(c_{\underline{\psi}}\right)_\Psi$

|  | -1 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|---|
| -1 | 7 | 0 | 2 | 7 | 7 | 4 | 7 | 2 | 2 |
| 0 | 5 | 0 | 3 | 7 | 3 | 3 | 1 | 0 | 0 |
| 1 | -1 | 6 | -1 | 2 | 4 | 2 | 6 | 3 | 5 |
| 2 | 2 | 3 | 1 | 5 | 7 | 2 | 5 | 7 | 0 |
| 3 | 5 | 1 | 2 | 3 | 5 | 6 | 6 | 5 | -1 |
| 4 | 5 | 6 | 1 | 1 | -1 | 7 | 2 | 4 | 2 |
| 5 | 0 | 2 | 2 | 7 | 2 | 2 | 5 | 4 | 3 |
| 6 | 6 | 1 | 1 | 5 | 2 | 6 | 1 | 3 | 5 |
| 7 | 6 | 0 | 4 | 2 | 6 | 0 | 0 | 3 | 7 |

Fig. 9. Numerical example of systematic encoding of the HCRS code $C^{\perp}(V_R, \Psi)$ by Algorithm 3, where $\Phi$ is given by (19) and the Gröbner basis $\mathcal{G}_\Phi$ is described in Example 14. By regarding $\left(h_{\underline{\psi}}\right)_{\Psi\setminus\Phi}$ as a received word with erasures, the negative redundant part $\left(-c_{\underline{\phi}}\right)_\Phi$ is obtained.

although we can choose $\Phi$ as

$$\Phi = \left\{ \begin{array}{c} (0,0),(1,0),(\alpha,0),(\alpha^2,0),(\alpha^3,0), \\ (\alpha^4,0),(\alpha^5,0),(\alpha^6,0),(0,1),(1,1), \\ (\alpha,1),(\alpha^2,1),(0,\alpha),(1,\alpha),(0,\alpha^2), \\ (1,\alpha^2),(0,\alpha^3),(0,\alpha^4),(0,\alpha^5),(0,\alpha^6) \end{array} \right\},$$

which has the same shape in $\Omega$ as $R \subseteq A$ because both $\Phi$ lead to $\det\left[\underline{x}_l\left(\underline{\phi}_m\right)\right] \neq 0$, we adopt (19) in order to show $\Phi$'s flexibility. The Gröbner basis $\mathcal{G}_\Phi = \left\{g^{(0)}, g^{(1)}, \cdots, g^{(8)}\right\}$ is then computed as

$$g^{(0)} = \alpha^4 + \alpha^2 x + \alpha^2 x^2 + \alpha^6 x^3 + x^4 + x^5 + \alpha^6 x^6 + x^7$$

$$+ \alpha^2 y + \alpha^6 y^2 + \alpha^6 y^3 + \alpha^4 y^4 + y^5 + \alpha^2 y^6 + y^7 + x^8,$$

$$g^{(1)} = \alpha^6 x + x^2 + \alpha^2 x^3 + \alpha^5 x^4 + \alpha^4 x^5 + \alpha x^6 + \alpha^3 x^7$$

$$+ \alpha^6 y + \alpha^5 x^2 y + \alpha x^3 y + \alpha^4 y^2 + \alpha^5 x y^2 + \alpha^2 y^3 + \alpha^5 x y^3$$

$$+ \alpha y^4 + y^5 + \alpha^5 y^6 + \alpha^3 y^7 + x^4 y,$$

$$g^{(2)} = \alpha^4 x + \alpha^2 x^2 + \alpha^5 x^3 + \alpha^7 x^5 + \alpha^4 y + \alpha^6 x y + \alpha^6 x^2 y$$

$$+ \alpha^4 x^3 y + \alpha^2 y^2 + \alpha^6 x y^2 + \alpha^5 y^3 + \alpha^4 x y^3 + \alpha^7 y^5 + x^2 y^2,$$

$$g^{(3)} = \alpha^6 x + \alpha^5 x^2 + \alpha x^3 + \alpha^2 x^4 + \alpha^5 x^5 + \alpha^2 x^6 + \alpha^6 y$$

$$+ x^2 y + \alpha x^3 y + \alpha y^2 + \alpha x y^2 + \alpha^3 y^3 + \alpha^5 x y^3 + \alpha^6 y^4$$

$$+ \alpha^3 y^5 + \alpha^6 y^6 + x^2 y^3,$$

$$g^{(4)} = \alpha^6 x + \alpha^4 x^2 + \alpha^2 x^3 + \alpha x^4 + x^5 + \alpha^5 x^6 + \alpha^3 x^7$$

$$+ \alpha^6 y + \alpha^5 x^2 y + \alpha^5 x^3 y + y^2 + \alpha^5 x y^2 + \alpha^2 y^3 + \alpha x y^3$$

$$+ \alpha^5 y^4 + \alpha^4 y^5 + \alpha y^6 + \alpha^3 y^7 + x y^4,$$

$$g^{(5)} = \alpha^3 x + \alpha^7 x^2 + x^3 + \alpha^4 x^4 + \alpha^2 x^5 + \alpha^4 x^7 + \alpha^3 y$$

$$
\begin{aligned}
&+\alpha^3x^2y+\alpha^3x^3y+\alpha^3y^2+\alpha^3xy^2+y^3+\alpha^5xy^3+\alpha y^4\\
&+\alpha^2y^5+y^6+\alpha^4y^7+xy^5,\\
&g^{(6)}=\alpha x+\alpha x^2+\alpha^2x^3+\alpha^2x^4+\alpha^7x^5+\alpha^4x^7+\alpha y\\
&+\alpha^3x^2y+\alpha^3x^3y+\alpha^5y^2+\alpha^2xy^2+\alpha^5y^3+\alpha^7xy^3\\
&+\alpha^6y^4+\alpha^7y^5+xy^6,\\
&g^{(7)}=1+\alpha x+\alpha^4x^2+\alpha^5x^4+\alpha^6x^6+\alpha^3x^7+\alpha y\\
&+\alpha^2xy+\alpha^7x^2y+\alpha^7x^3y+\alpha^3y^2+\alpha^7xy^2+\alpha^3xy^3\\
&+\alpha y^4+\alpha^2y^6+\alpha^3y^7+xy^7,\\
&g^{(8)}=\alpha^4+\alpha^2x+\alpha^6x^2+\alpha^6x^3+\alpha^4x^4+x^5+\alpha^2x^6\\
&+x^7+\alpha^2y+\alpha^2y^2+\alpha^6y^3+y^4+y^5+\alpha^6y^6+y^7+y^8.
\end{aligned}
$$

All values of Algorithm 3 are shown in Fig. 9. □

Thus, the systematic encoding can be viewed as a special case of Algorithm 2 for $\left(u_{\underline{\psi}}\right)_\Psi = \left(h_{\underline{\psi}}\right)_\Psi$ with $h_{\underline{\psi}} = 0$ for all $\underline{\psi} \in \Phi$. As there are many cases where the erasure-only correctable bound is exceeded, it is expected that both erasure-only and erasure-and-error can often be decoded beyond the erasure-and-error correcting bound $|\Phi_1|+2|\Phi_2| < d_{\mathrm{FR}}$. In [21], the improvement and the necessary and sufficient condition for generic erasure-and-error decoding to succeed are obtained for Hermitian codes.

*Remark 5:* If linear codes have non-trivial automorphism groups, then systematic encoding can also be performed by a division algorithm via Gröbner bases for modules [12],[16]. Indeed, there are cases where its computational complexity is less than that of Algorithm 3, as shown in [5],[34]. On the other hand, our method is more widely applicable to codes independent of automorphism groups. Another advantage of our method is that there are cases where encoding and erasure-and-error decoding are integrated, and thereby the overall size of the encoder and decoder is reduced; for the case of Reed–Solomon codes, see [20]. □

## VI. Estimation of Complexity

### A. Simple counting

We now estimate the number of finite-field operations, i.e., additions, subtractions, multiplications, and divisions, required by our method. We consider Algorithm 2 for the code $C^{\perp}(V_R,\Psi)$, as our systematic encoding algorithm corresponds to a special case of Algorithm 2. In this subsection, we simply count the operations in each step of the algorithm.

A summary of the results of our evaluation is given in Table I, where $n$ is the code length, $N$ is the dimension of $\Omega$, $q$ is the finite-field size, $b$ is the number of elements in the Gröbner bases, and Step 5 is decomposed into Step 5a of $\left(k_{\underline{a}}\right)_A = \mathcal{E}\left(\left(\widetilde{u}_{\underline{r}}\right)_R\right)$ and Step 5b of $\left(e_{\underline{\psi}}\right)_\Psi = \mathcal{R}\circ\mathcal{F}^{-1}\left(\left(k_{\underline{a}}\right)_A\right)$. We now consider the above estimation of each step.

TABLE I

NUMBER OF FINITE-FIELD OPERATIONS IN ALGORITHM 2

| Algorithm 2 | manipulation | order of bound |
|---|---|---|
| Step 1 | $\left(\sum_{\underline{\phi}\in\Phi_1}\underline{\phi}^{\underline{r}}\right)_R$ | $Nn^2$ |
| Step 2 | BMS | $bn^2$ |
| Step 3 | $\left(\sum_{\underline{\psi}\in\Psi}u_{\underline{\psi}}\underline{\psi}^{\underline{r}}\right)_R$ | $Nn^2$ |
| Step 4 | BMS | $bn^2$ |
| Step 5a | $\mathcal{E}\left(\left(\widetilde{u}_{\underline{r}}\right)_R\right)$ | $nq^N$ |
| Step 5b | $\mathcal{R}\circ\mathcal{F}^{-1}\left(\left(k_{\underline{a}}\right)_A\right)$ | $nNq^N$ |
| Step 6 | $\left(u_{\underline{\psi}}\right)_\Psi-\left(e_{\underline{\psi}}\right)_\Psi$ | $n$ |

Step 1) The calculation of DFT $\sum_{\underline{\phi}\in\Phi_1}\underline{\phi}^{\underline{r}}$ can be decomposed into updating $\underline{\phi}^{\underline{r}}$ and adding to the preserved value. This means that, at most, $N+1$ operations are repeated $|\Phi_1|$ times, so $(N+1)|\Phi_1|$ operations are required to compute one sum $\sum_{\underline{\phi}\in\Phi_1}\underline{\phi}^{\underline{r}}$. As there are at most $|\Psi|=n$ values on $R\subseteq D(\Psi)$, the total number of $\mathbb{F}_q$-operations in Step 1 has an upper bound of the order $Nn^2$.

Step 2) The computational complexity of the BMS algorithm [4],[7] is quoted as $bn^2$.

Step 3) Similarly to Step 1, the calculation of DFT $\sum_{\underline{\psi}\in\Psi}u_{\underline{\psi}}\underline{\psi}^{\underline{r}}$ can be decomposed into updating $\underline{\psi}^{\underline{r}}$, multiplying by $u_{\underline{\psi}}$, and adding to the preserved value. As these three operations are repeated $|\Psi|$ times, $(N+2)|\Psi|$ operations are required to compute one sum $\sum_{\underline{\psi}\in\Psi}u_{\underline{\psi}}\underline{\psi}^{\underline{r}}$. As there are at most $n$ values on $R$, the total number of $\mathbb{F}_q$-operations in Step 3 has an upper bound of the order $Nn^2$.

Step 4) The order $bn^2$ is quoted, as for Step 2.

Step 5a) For the extension of syndrome values, there are $2|D(\Psi)|=2|\Psi|$ additions and multiplications in the recurrence (8). Thus, the order of the upper bound for the extension is $nq^N$.

Step 5b) Similarly to Step 3, the calculation of $\mathcal{F}^{-1}$ can be decomposed into updating $\omega_{i_1}^{-l_1}\cdots\omega_{i_m}^{-l_m}$, summing $\sum_{J\subseteq[1,N]\setminus I}(-1)^{|J|}k_{\underline{i}(I,J)}$, multiplying, and adding to the preserved value. The total number is $\left(m+2^{N-m}+2\right)q^m$, which is bounded by $(N+3)q^N$. As these operations are repeated $n$ times, the total number of $\mathbb{F}_q$-operations in Step 5b has an upper bound of the order $nNq^N$.

Step 6) Exactly $|\Psi|=n$ subtractions are performed.

Because $N\leq b$, the total number of operations in Algorithm 2 has an upper bound of the order $bn^2+nNq^N$. If $N=1$, then we have $n\leq q$ and $bn^2+nNq^N\leq 2q^2$. Suppose that $N>1$. In the proof [8] of $\{$linear codes$\}=\{$affine variety codes$\}$, $q^N$ is chosen as $q^{N-1}<n\leq q^N$, which leads to $q^N<qn$ and $N-1<\log_q n\leq N$. Then, $bn^2+nNq^N$ has an upper bound of the order $n^2\left(b+q\log_q n\right)$; the factor $\left(b+q\log_q n\right)$ is comparatively less than $n$. Thus, Algorithm 2 improves the order $n^3$ of the total computational complexity of the erasure-and-error

TABLE II

NUMBER OF FINITE-FIELD OPERATION IN ALGORITHM 2 APPLIED AN M-D DFT ALGORITHM TO STEPS 1, 3, AND 5b

| Algorithm 2 | manipulation | order of bound |
|---|---|---|
| Step 1′ | $\left(\sum_{\underline{\phi}\in\Phi_1}\underline{\phi}^{\underline{a}}\right)_A$ | $Nq^{N+1}$ |
| Step 3′ | $\left(\sum_{\underline{\psi}\in\Psi}u_{\underline{\psi}}\underline{\psi}^{\underline{a}}\right)_A$ | $Nq^{N+1}$ |
| Step 5b′ | $\mathcal{F}^{-1}\left(\left(k_{\underline{a}}\right)_A\right)$ | $\begin{cases} Nq^{N+1} & N \le q \\ 2^N q^{N+1} & \text{general} \end{cases}$ |

decoding by the Gaussian elimination. Our method based on Main Lemma reduces the complexity of evaluating erasure-and-error values from $O(n^3)$ to $O(n^2 q \log_q n)$.

### B. Application of multidimensional DFT algorithm

In Steps 1, 3, and 5b of Algorithm 2, the computations of DFT and IDFT are restricted to values on $R$ and $\Psi$, respectively. In this subsection, we consider the algorithm that enlarges their computations to $A$ and $\Omega$, i.e., the algorithm that replaces Steps 1, 3, and 5b with the following.

Step 1′. $\left(v_{\underline{a}}\right)_A = \left(\sum_{\underline{\psi}\in\Phi_1}\underline{\psi}^{\underline{a}}\right)_A$

Step 3′. $\left(\widetilde{u}_{\underline{a}}\right)_A = \left(\sum_{\underline{\psi}\in\Psi}u_{\underline{\psi}}\underline{\psi}^{\underline{a}}\right)_A$

Step 5b′. $\left(e_{\underline{\omega}}\right)_\Omega = \mathcal{F}^{-1}\left(\left(k_{\underline{a}}\right)_A\right)$

If the complexity of Steps 1′, 3′, and 5b′ is estimated by the same method as for Steps 1, 3, and 5b, the result is an upper bound of the order $Nq^{2N}$. It is well-known that the computational complexity of the ordinary FFT is of the order $L \log L$, where $L$ is the size of the data. As $L = q^N$ in our case, $L \log L$ is equal to $Nq^N \log q$, though the ordinary FFT cannot be applied to our DFT and IDFT over the finite field. By applying a multidimensional (m-D) DFT algorithm [3], we find the computational complexities of Steps 1′, 3′, and 5b′ to be as shown in Table II.

First, we show by induction that the computational complexity of calculating $\mathcal{F}\left(\left(c_{\underline{\omega}}\right)_\Omega\right) = \left(\sum_{\underline{\omega}\in\Omega}c_{\underline{\omega}}\underline{\omega}^{\underline{a}}\right)_A$ is bounded by $3Nq^{N+1}$. For $N = 1$, we obtain the bound $3q^2$, as $\sum_{\omega\in\Omega}c_\omega\omega^a$ is decomposed into updating $\omega^a$, multiplying by $c_\omega$, and adding to the preserved value for all $\omega \in \Omega = \mathbb{F}_q$ and for all $a \in A = [0, q-1]$. Assume that, for $N-1$, we obtain the bound $3(N-1)q^N$. The summation can be decomposed as

$$\sum_{\omega_N\in\mathbb{F}_q}\omega_N^{a_N}\sum_{(\omega_1,\cdots,\omega_{N-1})\in\mathbb{F}_q^{N-1}}c_{(\omega_1,\cdots,\omega_{N-1},\omega_N)}\omega_1^{a_1}\cdots\omega_{N-1}^{a_{N-1}}. \tag{20}$$

By induction hypothesis, the complexity of the interior summation in (20) for all $a_1,\cdots,a_{N-1} \in [0,q-1]$ is bounded by $3(N-1)q^N$. For all $\omega_N \in \mathbb{F}_q$, the values of the interior summation are calculated in advance. The complexity of the exterior summation in (20) for all $a_N \in [0,q-1]$ is then bounded by $3q^2$, from the case of $N = 1$. As the exterior summation is carried out for all $a_1,\cdots,a_{N-1} \in [0,q-1]$, the total complexity of computing

$\mathcal{F}\left(\left(c_{\underline{\omega}}\right)_{\Omega}\right)$ is bounded by

$$3(N-1)q^N \times q + 3q^2 \times q^{N-1} = 3Nq^{N+1}.$$

Next, we estimate the complexity of calculating $\mathcal{F}^{-1}$ as follows. In (3), the values of $\sum_{J\subseteq[1,N]\setminus I}(-1)^{|J|}h_{\underline{i}(I,J)}$ are computed for all $1 \le l_1, \cdots, l_m < q$ in advance; the complexity is $2^{N-m}(q-1)^m$. Then, similarly to $\mathcal{F}$, the summation of $1 \le l_1, \cdots, l_m < q$ is computed with a complexity of $3m(q-1)^{m+1}$. As there are $\binom{N}{m}$ choices of $I \subseteq [1, N]$ such that $|I| = m$, the total complexity of computing $\mathcal{F}^{-1}$ is bounded by

$$\begin{aligned}
&\sum_{m=0}^{N}\binom{N}{m}\left\{2^{N-m}(q-1)^m + 3m(q-1)^{m+1}\right\}\\
&\le (q+1)^N + 3Nq^{N+1} = (1+1/q)^N q^N + 3Nq^{N+1}\\
&\le e^{N/q}q^N + 3Nq^{N+1}. \qquad (21)
\end{aligned}$$

If $N \le q$, then (21) has an upper bound of the order $Nq^{N+1}$, otherwise $2^N q^{N+1}$. Thus, it is strongly recommended, from the perspective of using the m-D DFT algorithm, that we should increase $q$ rather than $N$ in order to satisfy $q^{N-1} < n \le q^N$ for a given $n$. In the general case including $N > q$, we may choose either Steps 1, 3, and 5b or Steps 1′, 3′, and 5b′ in order to minimize the complexity of $nNq^N$ or (21).

On the other hand, as for Step 5a, we cannot apply the m-D DFT algorithm to the computation $\mathcal{E}\left(\left(\widetilde{u}_{\underline{r}}\right)_R\right)$, which has a complexity of order $nq^N$. However, note that the equality (8) that defines the extension $\mathcal{E}$ is almost identical to that of the discrepancy of the BMS algorithm. Actually, in the BMS algorithm, the discrepancy $\mathcal{D}_{\underline{a}}\left(g^{(w)}\right)$ of updating polynomial $g^{(w)} \in \mathbb{F}_q[\underline{x}]$ at $\underline{a} \in A$ is represented by

$$\mathcal{D}_{\underline{a}}\left(g^{(w)}\right) = k_{\underline{a}} + \sum_{\underline{d}\in D(\Psi)} g^{(w)}_{\underline{d}} k_{\underline{a}+\underline{d}-\underline{d}_w},$$

for which the summation is the same as in (8). Thus, the computation of $\mathcal{E}\left(\left(\widetilde{u}_{\underline{r}}\right)_R\right)$ in Step 5a can be considered as the extended part of the BMS algorithm, and does not cause serious damage in practice.

## VII. Conclusion

Conventionally, the m-D DFT and IDFT over $\mathbb{F}_q$ are seen as transforms between two vector spaces, each of which is indexed by $\left(\mathbb{F}_q^{\times}\right)^N$. In this paper, we have generalized these to transforms between two vector spaces, each of which is indexed by $\mathbb{F}_q^N$. Moreover, the Fourier inversion formulae of their transforms has also been generalized. We obtained a lemma using the linear recurrence relations from Gröbner bases and the generalized inverse transforms. This states that there is a canonical one-to-one linear map from a vector space indexed by the delta set of Gröbner bases onto another vector space indexed by an arbitrary subset of $\mathbb{F}_q^N$. As an application of our lemma, we have described the construction of affine variety codes, and have shown that the systematic encoding of a class of dual affine variety codes is nothing but a special case of erasure-only decoding. As another application of our lemma, we have proposed a fast error-value estimation in the erasure-and-error decoding of the class of dual affine variety codes. We have improved the computational complexity of the error-value estimation from $O(n^3)$ under Gaussian elimination to $O(qn^{2+\varepsilon})$ with any $0 < \varepsilon < 1$, where $n$ is the code length. Future work will concentrate on improving the error-correcting capability of generic erasure-and-error cases.

## Appendix A
## Proof of Proposition 1

It may be proved that, for $\left(c'_{\underline{\omega}}\right)_{\Omega} \in V_{\Omega}$, if $\left(k_{\underline{a}}\right)_A = \mathcal{F}\left(\left(c'_{\underline{\omega}}\right)_{\Omega}\right)$ and $\left(c_{\underline{\omega}}\right)_{\Omega} = \mathcal{F}^{-1}\left(\left(k_{\underline{a}}\right)_A\right)$ are defined, then $\left(c_{\underline{\omega}}\right)_{\Omega} = \left(c'_{\underline{\omega}}\right)_{\Omega}$ holds. [4] This is shown as follows, where we denote $\overline{\omega} = (-1)^m \omega_{i_1}^{-l_1} \cdots \omega_{i_m}^{-l_m}$.

$$\begin{aligned}
c_{\underline{\omega}} &= \sum_{l_1,\cdots,l_m=1}^{q-1} \left\{ \sum_{J \subseteq [1,N] \setminus I} (-1)^{|J|} k_{\underline{i}(I,J)} \right\} \overline{\omega} \\
&= \sum_{l_1,\cdots,l_m=1}^{q-1} \left\{ \sum_{J \subseteq [1,N] \setminus I} (-1)^{|J|} \sum_{\underline{\psi} \in \Omega} c'_{\underline{\psi}} \underline{\psi}^{\underline{i}(I,J)} \right\} \overline{\omega} \\
&= \sum_{l_1,\cdots,l_m=1}^{q-1} \left\{ \sum_{\underline{\psi} \in \Omega} c'_{\underline{\psi}} \left( \sum_{J \subseteq [1,N] \setminus I} (-1)^{|J|} \underline{\psi}^{\underline{i}(I,J)} \right) \right\} \overline{\omega} \\
&= \sum_{l_1,\cdots,l_m=1}^{q-1} \left\{ \sum_{\underline{\psi} \in \Omega,\, i \notin I \Rightarrow \psi_i = 0} c'_{\underline{\psi}} \psi_{i_1}^{l_1} \cdots \psi_{i_m}^{l_m} \right\} \overline{\omega} \qquad (22) \\
&= (-1)^m (q-1)^m c'_{\underline{\omega}} = c'_{\underline{\omega}}
\end{aligned}$$

At the conversion to (22), the following equality (23) has been used. For a given $\underline{\omega} \in \Omega$, let $I = I_{\underline{\omega}}$ be as in Definition 2. Then, for any $\underline{\psi} \in \Omega$,

$$\sum_{J \subseteq [1,N] \setminus I_{\underline{\omega}}} (-1)^{|J|} \underline{\psi}^{\underline{i}(I_{\underline{\omega}},J)} = \begin{cases} \psi_{i_1}^{l_1} \cdots \psi_{i_m}^{l_m} & \text{if } \psi_i = 0 \text{ for } \forall\, i \in [1,N] \setminus I_{\underline{\omega}} \\ 0 & \text{if } \exists\, i \in [1,N] \setminus I_{\underline{\omega}} \text{ with } \psi_i \neq 0. \end{cases} \qquad (23)$$

As $\underline{\psi}^{\underline{i}(I_{\underline{\omega}},J)} = \psi_{i_1}^{l_1} \cdots \psi_{i_m}^{l_m} \prod_{j \in J} \psi_j^{q-1}$, the equality (23) is proved by the following formula, which is known as a variant of the inclusion-exclusion principal [18],

$$\sum_{J \subseteq [1,N] \setminus I_{\underline{\omega}}} (-1)^{|J|} \prod_{j \in J} \psi_j^{q-1} = \prod_{i \in [1,N] \setminus I_{\underline{\omega}}} \left(1 - \psi_i^{q-1}\right). \quad \square$$

## Appendix B
## Proof of Proposition 2

From the assumption, we have

$$k_{\underline{d}} = \sum_{\underline{\psi} \in \Psi} \epsilon_{\underline{\psi}} \underline{\psi}^{\underline{d}}, \qquad (24)$$

[4] If $\mathcal{F}^{-1} \circ \mathcal{F} = \mathrm{id.}$, then $\mathcal{F}$ is injective and $\mathcal{F}^{-1}$ is surjective, and it follows from $\dim V_A = \dim V_{\Omega}$ that $\mathcal{F}$ and $\mathcal{F}^{-1}$ are isomorphic and that $\mathcal{F} \circ \mathcal{F}^{-1} = \mathrm{id.}$.

where $\underline{d} \in D = D(\Psi)$. We now show by induction that (24) holds not only for $\underline{d} \in D(\Psi)$, but also for $\underline{d} \in A$ if $\left(k_{\underline{a}}\right)_A$ satisfies the linear recurrence relation (8) from $\mathcal{G}_\Psi$. Actually, we have

$$\begin{aligned} k_{\underline{a}} &= -\sum_{\underline{d}\in D} g^{(w)}_{\underline{d}} k_{\underline{a}+\underline{d}-\underline{d}_w} = -\sum_{\underline{d}\in D} g^{(w)}_{\underline{d}} \sum_{\underline{\psi}\in\Psi} \epsilon_{\underline{\psi}} \underline{\psi}^{\underline{a}+\underline{d}-\underline{d}_w} \\ &= \sum_{\underline{\psi}\in\Psi} \epsilon_{\underline{\psi}} \underline{\psi}^{\underline{a}-\underline{d}_w} \left\{ -\sum_{\underline{d}\in D} g^{(w)}_{\underline{d}} \underline{\psi}^{\underline{d}} \right\} = \sum_{\underline{\psi}\in\Psi} \epsilon_{\underline{\psi}} \underline{\psi}^{\underline{a}}, \end{aligned}$$

where we use $-\sum_{\underline{d}\in D} g^{(w)}_{\underline{d}} \underline{\psi}^{\underline{d}} = \underline{\psi}^{\underline{d}_w}$, which follows from $g^{(w)}(\underline{\psi}) = 0$ in (6) for $\underline{\psi} \in \Psi$. Thus, (24) holds for all $\underline{d} = \underline{a} \in A$; in other words, $\left(k_{\underline{a}} = \sum_{\underline{\psi}\in\Psi} \epsilon_{\underline{\psi}} \underline{\psi}^{\underline{a}}\right)_A$ holds. □

## Appendix C

## Proof of Proposition 3

Consider an $n \times n$ matrix $\left[\underline{x}_l \left(\underline{\psi}_m\right)\right]$ whose $(l, m)$-th entry is equal to $\underline{x}_l \left(\underline{\psi}_m\right)$, where $\left\{\underline{x}^{\underline{d}} \,\middle|\, \underline{d} \in D(\Psi)\right\} = \{\underline{x}_l \mid 1 \leq l \leq n\}$ and $\Psi = \left\{\underline{\psi}_m \,\middle|\, 1 \leq m \leq n\right\}$ are aligned by any order with $n = |\Psi| = |D(\Psi)|$. The map $\mathrm{ev} : V_D \to V_\Psi$ of (5) can then be represented as

$$\left(h_{\underline{d}}\right)_D \mapsto \left(\sum_{\underline{d}\in D} h_{\underline{d}} \underline{\psi}^{\underline{d}}\right)_\Psi \Longleftrightarrow (h_l) \mapsto (h_l) \left[\underline{x}_l \left(\underline{\psi}_m\right)\right], \tag{25}$$

where $(h_l)$ represents any row vector of length $n$. Moreover, the map $\mathcal{P} : V_\Psi \to V_D$ of (9) can be represented as

$$\left(c_{\underline{\psi}}\right)_\Psi \mapsto \left(\sum_{\underline{\psi}\in\Psi} c_{\underline{\psi}} \underline{\psi}^{\underline{d}}\right)_D \Longleftrightarrow (c_l) \mapsto (c_l) \left[\underline{x}_m \left(\underline{\psi}_l\right)\right], \tag{26}$$

where $(c_l)$ represents any row vector of length $n$. These facts lead to Proposition 3 in case of the standard bases because $\left[\underline{x}_m \left(\underline{\psi}_l\right)\right]$ indicates the transpose matrix whose $(l, m)$-th entry is equal to $\underline{x}_m \left(\underline{\psi}_l\right)$.

Suppose that $\{v_1, \cdots, v_n\}$ and $\{v'_1, \cdots, v'_n\}$ are any two normal orthogonal bases of $V_D$ that consist of row vectors. Then there exists an $n \times n$ matrix $A$ with ${}^t(A^{-1}) = A$ such that $[v_i] = A[v'_i]$, where $[v_i]$ and $[v'_i]$ represent the matrices whose $i$-th row are equal to $v_i$ and $v'_i$ for all $1 \leq i \leq n$. Similarly, suppose that $\{w_1, \cdots, w_n\}$ and $\{w'_1, \cdots, w'_n\}$ are any two normal orthogonal bases of $V_\Psi$ that consist of row vectors. Then there exists an $n \times n$ matrix $B$ with ${}^tB = B^{-1}$ such that $[w_i] = B[w'_i]$. Thus the conditions (25) and (26) indicate that $(h_l)\, [\mathrm{ev}(v_i)] = (h_l)X$ and $(c_l)\, [\mathcal{P}(w_i)] = (c_l){}^tX$ with $X = \left[\underline{x}_l \left(\underline{\psi}_m\right)\right]$ if we take the standard bases $\{v_i\}$ and $\{w_i\}$ with the $n$-th identity matrix $[v_i] = [w_i]$. Suppose that $(h_l)\, [\mathrm{ev}(v'_i)] = (h_l)Y[w'_i]$ and $(c_l)\, [\mathcal{P}(w'_i)] = (c_l)Z[v'_i]$. Then we have

$$\begin{aligned} [\mathrm{ev}(v'_i)] &= YB^{-1} = A^{-1}\, [\mathrm{ev}\,(v_i)] = A^{-1}X, \\ [\mathcal{P}(w'_i)] &= ZA^{-1} = B^{-1}\, [\mathcal{P}\,(w_i)] = B^{-1}{}^tX. \end{aligned}$$

Thus we have $Y = A^{-1}XB$, $Z = B^{-1}{}^tXA$, and ${}^tY = Z$, which leads to Proposition 3 in case of any normal orthogonal bases. □

## APPENDIX D
## PROOF OF $C^{\perp}(U,\Psi) = \mathcal{C}\left(U^{\perp}\right)$

We show that, for all $\left(u_{\underline{\psi}}\right)_{\Psi} \in \mathrm{ev}(U)$ and all $\left(v_{\underline{\psi}}\right)_{\Psi} \in \mathcal{C}\left(U^{\perp}\right)$, the value of the inner product $\sum_{\underline{\psi}\in\Psi} u_{\underline{\psi}} v_{\underline{\psi}}$ is equal to zero. Let $(u_l)_{1\le l\le n}$ be the aligned $\left(u_{\underline{\psi}}\right)_{\Psi}$, as in Appendix C. By (25), $\left(u_{\underline{\psi}}\right)_{\Psi} \in \mathrm{ev}(U)$ is represented as

$$(u_l) = (h_l)\left[\underline{x}_l\left(\underline{\psi}_m\right)\right] \text{ for some } (h_l) \in U.$$

Similarly, let $(v_l)_{1\le l\le n}$ be the aligned $\left(v_{\underline{\psi}}\right)_{\Psi}$. As $\mathcal{C} = \mathcal{P}^{-1}$ and (26), $\left(v_{\underline{\psi}}\right)_{\Psi} \in \mathcal{C}\left(U^{\perp}\right)$ is represented as

$$(v_l) = (k_l)\left[\underline{x}_m\left(\underline{\psi}_l\right)\right]^{-1} \text{ for some } (k_l) \in U^{\perp}.$$

Because the transpose of the row vector $(u_l)$ is equal to a column vector $(u_m) = \left[\underline{x}_m\left(\underline{\psi}_l\right)\right](h_m)$, $\sum_{\underline{\psi}\in\Psi} u_{\underline{\psi}} v_{\underline{\psi}}$ is equal to

$$(v_l)(u_m) = (k_l)\left[\underline{x}_m\left(\underline{\psi}_l\right)\right]^{-1}\left[\underline{x}_m\left(\underline{\psi}_l\right)\right](h_m) = 0. \ \square$$

## REFERENCES

[1] H.E. Andersen, O. Geil, "Evaluation codes from order domain theory," *Finite Fields their Appl.*, vol.14, no.1, pp.92–123, Jan. 2008.

[2] E. Berlekamp, R. McEliece, H. van Tilborg, "On the inherent intractability of certain coding problems," *IEEE Trans. Inf. Theory,* vol.24, no.3, pp.384–386, May 1978.

[3] R.E. Blahut, *Theory and Practice of Error Control Codes,* Addison–Wesley, 1983.

[4] M. Bras-Amorós, M.E. O'Sullivan, "The correction capability of the Berlekamp–Massey–Sakata algorithm with majority voting," *Appl. Algebr. Eng. Commun. Comput.*, vol.17, no.5, pp.315–335, Oct. 2006.

[5] J.-P. Chen, C.-C. Lu, "A serial-in serial-out hardware architecture for systematic encoding of Hermitian codes via Gröbner bases," *IEEE Trans. Commun.*, vol.52, no.8, pp.1322–1331, Aug. 2004.

[6] D. Cox, J. Little, D. O'Shea, *Ideals, Varieties, and Algorithms: An introduction to computational algebraic geometry and commutative algebra,* 2nd ed. New York: Springer Publishers, 1997.

[7] D. Cox, J. Little, D. O'Shea, "The Berlekamp–Massey–Sakata algorithm," *Using Algebraic Geometry,* 2nd ed., Chapter 10, pp.494–532, Springer, 2005.

[8] J. Fitzgerald, R.F. Lax, "Decoding affine variety codes using Gröbner bases," *Designs Codes Cryptogr.*, vol.13, no.2, pp.147–158, Feb. 1998.

[9] O. Geil, T. Høholdt, "On hyperbolic codes," in *Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes: Proc. AAECC-14,* S. Boztaş and I.E. Shparlinski, eds., no.2227 in *Lecture Notes in Computer Science,* pp.159–171, Springer-Verlag Berlin Heidelberg, 2001.

[10] O. Geil, R. Pellikaan, "On the structure of order domains," *Finite Fields Appl.*, vol.8, no.3, pp.369–396, Jul. 2002.

[11] O. Geil, "Evaluation codes from an affine variety code perspective," *Advances In Algebraic Geometry Codes,* E. Martinez-Moro, C. Munuera, D. Ruano, eds., World Scientific Publishing Co. Pte. Ltd., pp.153–180, 2008.

[12] C. Heegard, J. Little, K. Saints, "Systematic encoding via Gröbner bases for a class of algebraic-geometric Goppa codes," *IEEE Trans. Inf. Theory,* vol.41, no.6, pp.1752–1761, Nov. 1995.

[13] T. Høholdt, J. H. van Lint, R. Pellikaan, "Algebraic geometry codes," *Handbook of Coding Theory,* V. S. Pless and W. C. Huffman, eds., vol.1, pp.871–961, Elsevier, Amsterdam 1998.

[14] R. Kötter, "A fast parallel implementation of a Berlekamp–Massey algorithm for algebraic-geometric codes," *IEEE Trans. Inf. Theory,* vol.44, no.4, pp.1353–1368, Jul. 1998.

[15] J.B. Little, "The key equation for codes from order domains," *Advances In Coding Theory And Cryptography,* pp.1–17, T. Shaska *et al.*, eds., World Scientific Publishing Co. Pte. Ltd., 2007.

[16] J.B. Little, "Automorphisms and encoding of AG and order domain codes," *Gröbner Bases, Coding, and Cryptography,* pp.107–120, M. Sala *et al.*, eds., Springer Berlin Heidelberg, 2009.

[17] C. Marcolla, E. Orsini, M. Sala, “Improved decoding of affine-variety codes,” *J. Pure Appl. Algebr.,* vol.216, issue 7, pp.1533–1565, Jul. 2012.

[18] J. Matoušek, J. Nešetřil, *Invitation to Discrete Mathematics,* Oxford Univ. Press, 1998.

[19] H. Matsui, S. Mita, “Encoding via Gröbner bases and discrete Fourier transforms for several types of algebraic codes,” *IEEE Int. Symp. Inf. Theory,* pp.2656–2660, Nice, France, Jun. 24–29, 2007.

[20] H. Matsui, S. Mita, “A new encoding and decoding system of Reed–Solomon codes for HDD,” *IEEE Trans. Magn.,* vol.45, no.10, pp.3757–3760, Oct. 2009.

[21] H. Matsui, “Unified system of encoding and decoding erasures and errors for algebraic geometry codes,” *Int. Symp. on Inf. Theory and its Applications,* Taichung, Taiwan, pp.1001–1006, Oct. 17–20, 2010.

[22] H. Matsui, “Decoding a class of affine variety codes with fast DFT,” *Int. Symp. on Inf. Theory and its Applications,* Honolulu, Hawaii, USA, pp.436–440, Oct. 28–31, 2012.

[23] R. Matsumoto, S. Miura, “On the Feng-Rao bound for the L-construction of algebraic geometry codes,” *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.,* vol.E83–A, no.5, pp.923–926, May 2000.

[24] S. Miura, “Linear codes on affine algebraic varieties,” (in Japanese) *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.,* vol.J81–A, no.10, pp.1386–1397, Oct. 1998.

[25] R. Pellikaan, B.-Z. Shen, G.J.M. van Wee, “Which linear codes are algebraic-geometric?” *IEEE Trans. Inf. Theory,* vol.37, no.3, pp.583–602, May 1991.

[26] R. Pellikaan, “On decoding by error location and dependent sets of error positions,” *Discrete Math.,* vol.106/107, pp.369–381, Sep. 1992.

[27] D. Ruano, “Computing the Feng-Rao distances for codes from order domains,” *J. Algebra,* vol.309, issue 2, pp.672–682, Mar. 2007.

[28] K. Saints, C. Heegard, “On hyperbolic cascaded Reed–Solomon codes,” in *Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes: Proc. AAECC-10,* G. Cohen, T. Mora, and O. Moreno, eds., no.673 in *Lecture Notes in Computer Science,* pp.291–303, Berlin, Germany: Springer, 1993.

[29] K. Saints, C. Heegard, “Algebraic-geometric codes and multidimensional cyclic codes: a unified theory and algorithms for decoding using Gröbner bases,” *IEEE Trans. Inf. Theory,* vol.41, no.6, pp.1733–1751, Nov. 1995.

[30] S. Sakata, H.E. Jensen, T. Høholdt, “Generalized Berlekamp–Massey decoding of algebraic geometric codes up to half the Feng–Rao bound,” *IEEE Trans. Inf. Theory,* vol.41, no.6, Part I, pp.1762–1768, Nov. 1995.

[31] S. Sakata, D.A. Leonard, H.E. Jensen, T. Høholdt, “Fast erasure-and-error decoding of algebraic geometry codes up to the Feng–Rao bound,” *IEEE Trans. Inf. Theory,* vol.44, no.4, pp.1558–1564, Jul. 1998.

[32] G. Salazar, D. Dunn, S. B. Graham, “An improvement of the Feng–Rao bound on minimum distance,” *Finite Fields their Appl.* vol.12, issue 3, pp.313–335, Jul. 2006.

[33] H. Stichtenoth, *Algebraic Function Fields and Codes,* Springer-Verlag, 1993.

[34] V.T. Van, H. Matsui, S. Mita, “Computation of Gröbner basis for systematic encoding of generalized quasi-cyclic codes,” *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.,* vol.E92–A, no.9, pp.2345–2359, Sep. 2009.

**Hajime Matsui** received a B.S. degree in 1994 from the Department of Mathematics, Shizuoka University, Japan, an M.S. degree in 1996 from the Graduate School of Science and Technology, Niigata University, Japan, and Ph.D. in 1999 from the Graduate School of Mathematics, Nagoya University, Japan. From 1999 to 2002, he was a Postdoctorate Fellow in the Department of Electronics and Information Science at the Toyota Technological Institute, Japan. From 2002 to 2006, he was a Research Associate at the same institute, where he has been working as an Associate Professor since 2006. His research interests include coding theory, computer science, and number theory.